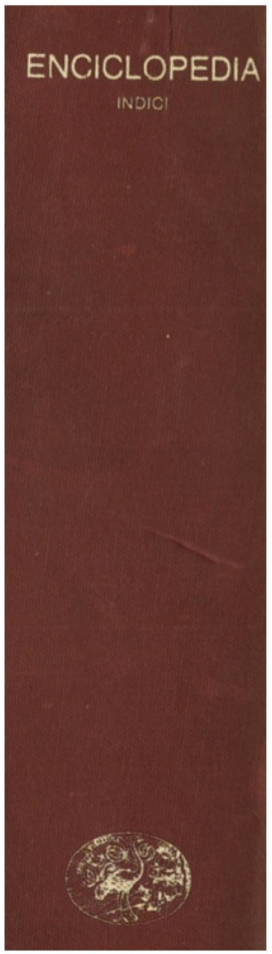


ENCICLOPEDIA EINAUDI [1982]

CALCOLO

Giulio Giorello e Marco Mondadori - **CALCOLO** pag.4

Walter Endrei - **ABACO** pag.14
Antoni Mazurkiewicz - **ALGORITMO** pag.22
Massimo Galuzzi, Krzysztof Moszyński, Andrej Wakulicz - **APPROSSIMAZIONE** pag.28
Giuseppe Geymonat e Giulio Giorello - **CALCOLO** pag.42
Giulio Giorello e Marco Mondadori - **NUMERO** pag.103
Giulio Giorello - **ZERO** pag.122

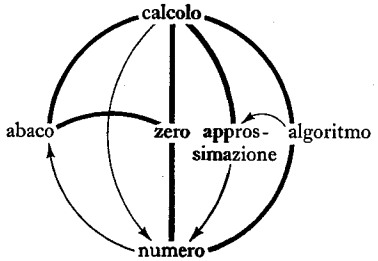
	anthropos	argomentazione	arti	calcolo	capitale	cervello	civiltà	classi	cognizione	combinatoria	comunicazione	concetto	conoscenza	corpo	creatività	cultura mat.
abaco	·	·	·	5	·	·	·	·	·	·	3	·	·	·	·	·
algoritmo	2	·	·	6	1	·	·	·	2	7	·	2	4	·	3	·
approssimazione	·	·	·	6	3	·	2	·	·	2	·	3	2	·	3	·
calcolo	2	4	3	7	6	3	3	·	3	7	5	4	5	·	2	4
numero	·	2	4	8	2	·	·	·	5	8	4	5	6	2	2	·
zero	·	·	·	4	3	·	·	·	·	·	5	·	·	2	·	·

	memoria	metodo	modo di produz.	mythos/logos	natura	normale/anormale	orale/scritto	organico/inorgan.	organismo	parentela	politica	probabilità	produzione/distrib.	regione	religione	rito
abaco	3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
algoritmo	·	5	·	·	·	·	3	·	·	·	·	·	·	·	·	·
approssimazione	·	3	·	·	·	·	·	3	·	·	·	·	·	·	·	·
calcolo	4	7	3	·	5	·	4	3	3	4	2	7	5	3	1	2
numero	2	6	·	3	6	·	4	2	3	·	3	8	3	3	·	·
zero	·	3	·	·	2	·	3	2	·	·	·	6	·	·	·	·

	calcolo	zero	abaco	numero	algoritmo	approssimazione
calcolo	·	6	5	5	2	3
zero	3	·	4	3	·	·
abaco	3	4	·	·	·	·
numero	·	6	3	·	2	·
algoritmo	6	·	·	3	·	1
approssimazione	6	·	·	4	·	·

	dialettica	domesticam.	eccedente	enunciazione	eredità	esoterico/essoter.	evoluzione	filosofia/filosofie	fisica	generazioni	geometria e topol.	giustizia	guerra	homo	inconscio	letteratura	linguaggio	locale/globale	logica	macchina	materia
abaco	3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	4	·
algoritmo	4	·	·	·	·	·	·	·	4	·	3	·	·	·	·	·	·	6	6	6	·
approssimazione	·	·	·	·	2	·	·	·	6	·	5	·	·	·	·	·	2	6	3	2	4
calcolo	7	·	2	·	2	3	2	5	8	·	7	·	2	·	1	·	5	9	7	8	5
numero	7	·	·	3	2	4	2	3	7	·	8	3	·	·	·	·	4	8	8	6	7
zero	5	·	·	·	·	·	1	·	5	·	6	·	·	·	·	·	·	6	6	4	3

	sacro/profano	segno	sistema	società	soma/psiche	spiegazione	stato	storia	strutture matem.	sviluppo/sottosvil.	tempo/temporalità	teoria/modello	testo	tolleranza/intoll.	tonale/atonale	tradizioni	universo	uomo	visione	vita/morte
abaco	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
algoritmo	·	3	3	·	·	·	·	2	7	·	·	·	3	·	·	·	·	3	·	·
approssimazione	·	4	4	3	·	4	2	·	6	·	·	6	·	2	·	·	3	·	·	·
calcolo	·	6	5	4	2	6	·	4	7	·	4	5	1	·	·	2	6	5	4	·
numero	1	5	5	4	·	4	·	2	9	·	4	6	1	2	·	3	4	·	·	2
zero	2	·	2	2	·	4	·	3	6	·	·	5	·	·	·	·	·	2	·	·



Calcolo

ambiguità
competenza/esecuzione
fonetica
grammatica
lessico
lingua
lingua/parola
linguaggio
metrica
semantica
senso/significato
traduzione
universali/particolari

concetto
esistenza
essere
fenomeno
forma
idea
proposizione e giudizio

analogia e metafora
argomentazione
interpretazione

astratto/concreto
dialettica
identità/differenza
mediazione
opposizione/contraddizione
qualità/**quantità**
totalità
uno/molti

atti linguistici
dicibile/indicibile
enunciazione
presupposizione e allusione
referente

comunicazione
errore
informazione

decisione
distribuzione statistica
giochi
induzione statistica
probabilità
rappresentazione statistica
teoria/pratica

dato
etica
filosofia/filosofie
ragione
razionale/irrazionale
soggetto/oggetto
uguaglianza
valori
vero/falso
volontà

catastrofi
ciclo
evento
periodizzazione
tempo/temporalità

antico/moderno
calendario
decadenza
escatologia
età mitiche
genesi
passato/presente
progresso/reazione
storia

caos/cosmo
infinito
macrocosmo/microcosmo
mondo
natura
osservazione
reale
unità

curve e superfici
geometria e topologia
invariante

alchimia
astrologia
cabala
elementi
esoterico/essoterico

atlante
collezione
documento/monumento
fossile
memoria
rovina/restauro

armi
frontiera
guerra
imperi
nazione
tattica/strategia

deduzione/prova
equivalenza
formalizzazione
logica
possibilità/necessità
referenza/verità
ricorsività

differenziale
funzioni
infinitesimale
focale/globale
sistemi di riferimento
stabilità/instabilità
variazione

analisi/sintesi
anticipazione
ipotesi
matematiche
metodo

funzione
misura
modello
struttura
teoria/modello

alienazione
coscienza/autocoscienza
immaginazione sociale
pace
servo/signore
uomo
utopia

demagogia
discriminazione
repressione
terrore
tolleranza/intolleranza
tortura
violenza

centrato/acentrato
combinatoria
grafo
labirinto
rete

applicazioni
assioma/postulato
continuo/discreto
dipendenza/indipendenza
divisibilità
dualità
insieme
razionale/algebrico/trascendente
simmetria
strutture matematiche
trasformazioni naturali / categorie

abaco
algoritmo
approssimazione
calcolo
numero
zero

caso/probabilità
causa/effetto
certezza/dubbio
coerenza
convenzione
determinato/indeterminato
empiria/esperienza
esperimento
legge
libertà/necessità
metafisica
naturale/artificiale
operatività
paradigma
previsione e possibilità
riduzione
ripetizione
scienza
spiegazione
verificabilità/falsificabilità

categorie/categorizzazione
conoscenza
coppie filosofiche
disciplina/discipline
enciclopedia
innovazione/scoperta
insegnamento
invenzione
rappresentazione
ricerca
sistematica e classificazione

controllo/retroazione
energia
equilibrio/squilibrio
interazione
ordine/disordine
organizzazione
semplice/complesso
sistema
soglia
vincolo

analogico/digitale
automa
intelligenza artificiale
macchina
programma
simulazione
strumento

cervello
comportamento
e condizionamento
controllo **sociale**
emozione/motivazione
mente

apprendimento
autoregolazione/equilibrazione
cognizione
induzione/deduzione
innato/acquisito
istinto
operazioni
percezione
quoziente intellettuale

astronomia
cosmologie
gravitazione
luce
materia
spazio-tempo

atmosfera
litosfera
oceani
pianeti
sole
universo

atomo e molecola
conservazione/invarianza
entropia
fisica
forza/campo
moto
particella
plasma
propagazione
quanti
relatività
reversibilità/irreversibilità
stato fisico

adattamento
evoluzione
mutazione/selezione
polimorfismo
specie

cellula
differenziamento
immunità
individualità biologica
integrazione
invecchiamento
organismo
regolazione
sviluppo e morfogenesi

catalisi
macromolecole
metabolismo
omeostasi
organico/inorganico
osmosi
vita

eredità
gene
genotipo/fenotipo
razza
sangue

allegoria
codice
immagine
metafora
segno
significato
simbolo

avanguardia
classico
critica
filologia
letteratura
maniera
poetica
retorica

bello/brutto
creatività
espressione
fantastico
gusto
imitazione
immaginazione
progetto
riproduzione/riproducibilità
sensibilità
spazialità

anthropos
cultura/culture
etnocentrismi
natura/cultura

alfabeto
ascolto
gesto
lettura
luogo comune
orale/scritto
parola
ritmo
scrittura
voce

discorso
finzione
generi
narrazione/**narratività**
stile
tema/motivo
testo

arti
artigianato
artista
attribuzione
oggetto
produzione artistica

acculturazione
civiltà
futuro
selvaggio/barbaro/civilizzato

armonia
melodia
ritmica/metrica
scala
suono/rumore
tonale/atonale

colore
disegno/progetto
visione

escrementi
fertilità
nascita
sensi
sessualità
vecchiaia
vita/morte

abbigliamento
canto
corpo
danza
maschera
moda
ornamento
scena

amore
desiderio
eros
isteria
pulsione
soma/psiche
sonno/sogno

educazione
generazioni
infanzia
morte

coltivazione
cultura materiale
industria rurale
materiali
prodotti

credenze
dialetto
enigma
fiaba
mostro
popolare
proverbi
tradizioni

cannibalismo
dèi
divino
eroi
iniziazione
magia
messia
millennio
persona
puro/impuro
religione
sogno/visione
stregoneria

angoscia/colpa
castrazione e complesso
censura
identificazione e transfert
inconscio
nevrosi/psicosi
piacere

clinica
cura/normalizzazione
esclusione/integrazione
farmaco/droga
follia/delirio
medicina/medicalizzazione
normale/anormale
salute/malattia
sintomo/diagnosi

fuoco
homo
mano/manufatto
tecnica
utensile

ateo
chierico/laico
chiesa
diavolo
eresia
libertino
libro
peccato
sacro/profano
santità

demoni
divinazione
mito/rito
mythos/logos
origini

agonismo
cerimoniale
festa
feticcio
gioco
lutto
regalità
rito

casta
donna
endogamia/esogamia
famiglia
incesto
maschile/femminile
matrimonio
parentela
totem
uomo/donna

alimentazione
animale
cucina
domesticamento
fame
vegetale

borghesi/borghesia
burocrazia
classi
contadini
ideologia
masse
proletariato
rivoluzione

economia
formazione economico-sociale
lavoro
modo di produzione
proprietà
riproduzione
transizione

caccia/raccolta
dono
eccedente
pastorizia
primitivo
reciprocità/ridistribuzione

consenso/dissenso
egemonia/dittatura
intellettuali
libertà
maggioranza/minoranza
partiti
politica

amministrazione
comunità
conflitto
élite
gergo
gruppo
marginalità
opinione
povertà
propaganda
ruolo/status
socializzazione
società
spazio sociale

accumulazione
capitale
crisi
distribuzione
fabbrica
gestione
imperialismo
impresa
mercato
merce
moneta
pianificazione
profitto
rendita
salario
utilità
valore/plusvalore

abbondanza/scarsità
bisogno
consumo
imposta
lusso
oro e **argento**
pesi e **misure**
produzione/distribuzione
ricchezza
scambio
spreco

consuetudine
diritto
giustizia
istituzioni
responsabilità

costituzione
democrazia/**dittatura**
norma
patto
potere
potere/**autorità**
pubblico/**privato**
società **civile**
stato

abitazione
acqua
ambiente
città
clima
ecumene
insediamento
migrazione
paesaggio
popolazione
regione
risorse
suolo
terra
territorio
villaggio

agricoltura
città/campagna
colonie
commercio
industria
spazio **economico**
sviluppo/sottosviluppo

Calcolo

Abaco, Algoritmo, Approssimazione, Calcolo, Numero, Zero

riapparizione del caso, degli dèi (infinitamente piccoli... immaginari).
calcolo di Fermat.
esempio di Tantalo, nelle *Regulae*; applicabile a scoperte matematiche.
in questo universo cristallino della matematica vengono tese alla ragione le *stesse* trappole che nel mondo reale (Simone Weil).

1. *La «libertà» del matematico.*

1.1. Calcolo e procedure meccaniche.

Nel *De corpore* (1655) cosí si esprimeva Thomas Hobbes: «Per ragionamento io intendo ✦calcolo✦. Ora, calcolare significa o *effettuare la somma di molte cose che vengono aggiunte l'una all'altra*, o *sapere ciò che rimane quando una cosa viene tolta da un'altra*. Ragionamento, quindi, è la stessa cosa che *addizione* e *sottrazione*».

Lo storico della logica Joseph M. Bocheński nella sua *Logica formale* (*Formale Logik*, 1956) scorge in queste parole «piuttosto il *jeu d'esprit* di un dilettante che una teoria logico-matematica»: nessuna inferenza può venir interpretata a questo modo. Ma il passo hobbesiano contiene una forte immagine: quella della *ragione come calcolo*. Un'immagine che si innesta su una pratica che vanta una lunghissima tradizione di successi.

Questa pratica è ormai abbastanza familiare, almeno nei suoi elementi di base. Buona parte dell'insegnamento delle matematiche nella scuola consiste del resto nella presentazione e nell'esercizio di metodi di calcolo. Prima con le quattro operazioni fondamentali s'impara a ottenere somma, prodotto, differenza e quoziente di due numeri; seguono poi l'elevazione a potenza, l'estrazione di radice, la soluzione di equazioni lineari... Quel che c'è *di comune* in tutte queste procedure computazionali può venir individuato nel fatto che esse non coinvolgono nulla piú che l'applicazione meccanica di un insieme finito di istruzioni per manipolare simboli su carta. In linea di principio una macchina potrebbe svolgere le stesse operazioni con altrettanto successo.

La caratterizzazione del metodo nella «ricerca della verità» non poteva che risentire del «fascino discreto» del calcolo coi numeri. Dopo Hobbes, Leibniz: «Il vero metodo dovrebbe fornirci un *filum Ariadnes*, cioè un mezzo concreto e percepibile con i sensi che serva di guida alla mente, come... le forme delle operazioni che sono insegnate agli allievi in aritmetica... Per scoprire e dimostrare verità è necessaria l'analisi delle idee... che corrisponde all'analisi dei caratteri

[scritti]. Possiamo perciò rendere percepibile con i sensi l'analisi delle idee e guidarla come con un filo meccanico, perché l'analisi dei caratteri è un qualche cosa di percepibile con i sensi. [Ci occorre dunque] una *caratteristica* della *ragione*, mediante la quale le verità, in qualsiasi dominio, si presenterebbero alla ragione in virtú di un metodo di calcolo come nell'aritmetica e nell'algebra, purché essa si sottoponga al corso della deduzione. Di conseguenza, quando sorgeranno controversie fra due filosofi, non sarà piú necessaria una discussione, come [non lo è] fra due calcolatori. Sarà sufficiente, infatti, che essi prendano in mano le penne, si siedano di fronte agli abachi e (se cosí piace, su invito di un amico) si dicano l'un l'altro: *Calculemus!*»

Sul progetto leibniziano si tornerà piú oltre (in particolare alle pp. 47-48): preme per intanto a chi scrive insistere sul fatto che, si tratti di calcoli aritmetici e algebrici o di «calcoli logici» – come le parole di Leibniz suggeriscono – è insita nel procedimento computazionale un'idea di necessità che gli stessi termini – macchine, procedura meccanica, ecc. – evocano. In *La science et l'hypothèse* (1902) il grande matematico Henri Poincaré affermava che la stessa «invenzione matematica» rispecchiava la tradizionale antinomia di «necessità» e «volontà». La creatività (matematica) non sfugge ai suoi vincoli: quando il matematico – proseguiva Poincaré – formula i postulati di una teoria, proponendo un sistema assiomatico, viene a collocarsi esattamente in quel punto in cui la libertà dell'invenzione si salda con il carattere di rigorosa necessità della catena di successive deduzioni.

1.2. Due piú due fa davvero quattro?

Lo spirito, avrebbe detto Simone Weil nei *Cahiers*, «è schiavo ogniqualvolta accetta legami *non stabiliti* da lui». Ma nel calcolo, qual è la fonte dei legami? Con Alexander Pope potremmo anche noi chiederci: «Perché mai, o dèi, due piú due *dovrebbe* far quattro?»

Al proposito vale la pena di riportare un argomento di Félix, recentemente ripreso da vari autori. S'immagini di entrare in un negozio e di chiedere la consegna di due oggetti ciascuno del peso di due chilogrammi; essi vengono consegnati in una scatola che pesa a sua volta un chilo; in questa confezione due chili e due chili «fanno» *cinque* chili. È facile obiettare che l'operazione per cui «2 piú 2 è uguale a 5» non è un'addizione nel senso *abitualmente* inteso. Ma l'addizione abituale «$2+2=4$» non è che *un caso particolare* dell'addizione «con confezione»: i due oggetti, ciascuno del peso di due chili, vengono confezionati in modo che il peso della «confezione», dell'«involucro», sia zero. Si tornerà su questo modo di prospettare le cose.

1.3. Gli «universi» del calcolo.

Quanto detto piú sopra mostra come fin le piú apparenti e banali «verità» relative al «calcolo coi numeri» rappresentino delle conquiste. Come è una conquista la stessa *successione dei numeri naturali* (1, 2, 3, 4, 5, 6, ecc.) che rappresenta una delle situazioni matematiche piú di base e corrisponde all'operazione psicologica del *contare*. Ora, alcune culture non realizzano che l'operazione del contare può venire prolungata *quanto si vuole*. Eppure l'universo matematico di queste culture «primitive» (per esempio, nulla, uno, due, tre, molti) è una struttura perfettamente consistente, anche se oggi una matematica in cui $0+0=0$, $0+1=1$, $1+1=2$, $0+2=2$, $2+2=4$ cioè *molti*, siano le uniche leggi sembra piuttosto povera. D'altra parte è bene tener presente che la stessa assimilazione dell'1 e del 2 agli altri «numeri» è conquista relativamente recente (del pensiero matematico del Rinascimento: cfr. l'articolo «Numero», § 1): i pitagorici – ma anche molti autorevoli pensatori successivi, per esempio Aristotele – ritenevano che l'*unità* (la *monade*) andasse distinta dai «numeri», essendone semmai «il generatore». Alcuni distinguevano dai «numeri» anche il 2 (la *diade*): né va dimenticato che il termine greco per numero, ἀριθμός, sembra indicare per lo piú una *pluralità* d'individui: si è resa necessaria una notevole *tensione* del concetto di ◆numero◆ per cancellare distinzioni di questo tipo. Le cose si sono svolte in modo ancor piú tortuoso per quanto riguarda lo ◆zero◆: oggi si è soliti inserire lo zero tra i numeri naturali ogni volta che ci fa comodo (si tratta di un simbolo essenziale per la scrittura dei numeri, una volta adottata una notazione posizionale come la per noi abituale notazione decimale). Ma lo zero è assente in molte altre culture, anche matematicamente progredite: progredite, per esempio, al punto di disporre di strumenti – come l'◆abaco◆ – che consentono di eseguire le quattro operazioni fondamentali fino ad ordini di grandezza *praticamente illimitati* che anticipano inconsapevolmente il concetto di notazione posizionale, *senza tuttavia che tale concetto venga necessariamente applicato nella numerazione scritta*.

È sostanzialmente nella realizzazione da parte dei matematici indiani di una scrittura posizionale decimale che compare anche un «simbolo per il nulla», l'antenato appunto del nostro zero; ed è grazie alla mediazione araba che l'Occidente cristiano ha potuto apprendere nel medioevo l'impiego di tali cifre, zero incluso (cfr. l'articolo ◆Zero◆, §§ 3.4-3.6 e 4).

2. *La «statua di Tantalo».*

2.1. Ampliare il dominio numerico.

Ma, oltre al sistema dei numeri naturali (zero incluso), che verrà denotato d'ora in poi con **N**, ci sono altre specie di numeri: ogni manuale di matematica presenta d'abitudine il sistema degli interi relativi **Z**; quello dei razionali, **Q**, quello dei reali, **R**; infine quello dei complessi, **C**. In che senso queste diverse strutture vengono accomunate dalla parola ◆numero◆? La risposta passa attraverso la disamina delle motivazioni, emerse nella pratica del calcolo, ad «ampliare» il dominio numerico inizialmente costituito dai soli naturali.

Un primo punto è costituito dal fatto che il sistema **N** non è chiuso rispetto alle inverse di addizione e moltiplicazione. Per esempio: il rapporto di due nu-

meri naturali non è necessariamente un numero naturale. Di qui l'emergenza, nella stragrande maggioranza delle varie culture matematiche, delle cosiddette *frazioni*. Ma, anche qui, la costituzione del «sistema delle frazioni» non è stata qualcosa di immediato. Nelle sue ormai classiche *Lezioni sulla storia delle scienze matematiche classiche* (*Vorlesungen über Geschichte der antiken matematischen Wissenschaften*, 1934) lo storico Neugebauer sottolinea come nella lingua dell'antico Egitto non esistano simboli per frazioni come 17/25, mentre per frazioni come 1/20, 1/25, ecc. esistono soltanto simboli ove il numeratore 1 non compare; per 1/2, infine, si fa uso di un segno del tutto diverso da quelli che indicano le altre frazioni. Queste differenze a livello della *notazione* sono tutt'altro che irrilevanti: con tutta probabilità attestano che, in tempi ancor piú antichi, frazioni come 1/2, 1/3, 2/3 venivano riguardate come numeri a sé, e non quali formazioni secondarie ottenute da coppie di numeri naturali. Ancora una volta – come nel caso dell'1 o del 2 per **N** – devono essere state ovvie esigenze calcolistiche a indirizzare verso una maggiore uniformità.

2.2. Il caso dei negativi.

Piú tormentata ancora la vicenda concernente i numeri «relativi» o «con segno». Regole come «meno per meno fa piú», che ancor oggi lasciano perplesso qualche studente, parevano straordinarie a quegli algebristi del Rinascimento che avevano appreso, tramite la mediazione araba, il calcolo di «crediti, debiti e nulla» sviluppato a suo tempo dagli Indiani. Ancora un matematico come Lazare Carnot, l'autore delle *Réflexions sur la métaphysique du calcul infinitésimal* (1797), dichiarava che l'idea che esistessero numeri *negativi*, «quantità minori del nulla» (cioè di *zero*), era assurda: i numeri negativi altro non erano che «utili finzioni» (*numeri ficti* erano comunemente chiamati dagli algebristi cinquecenteschi!) che andavano *introdotte* e poi *eliminate* nella soluzione dei problemi per mere esigenze di calcolo.

Fu solo nell'Ottocento che si produsse una ricostruzione *rigorosa* del calcolo in **Z** e di quello in **Q** concependoli entrambi come calcoli di coppie (per le «regole» di tali calcoli vedi, per esempio, «Calcolo», § 2.8). Nei vari articoli di questa *Enciclopedia* si è in particolare presentato il calcolo in **Z** come un calcolo di coppie di elementi di **N** e quindi il calcolo in **Q** come calcolo di coppie di elementi di **Z**. Si sarebbe potuto (il che è meno abituale ma piú vicino all'*iter* storico effettivo) introdurre prima i razionali senza segno come coppie di elementi di **N** e successivamente i numeri «con segno» come coppie di razionali «senza segno», ottenendosi alla fine un corpo isomorfo al corpo **Q** ottenuto coll'*iter* precedente (per la nozione di *corpo* o *campo* si veda per esempio «Calcolo», § 2.4). Ma, quale delle due vie si segua, resta il fatto che l'effettivo processo storico ha conosciuto non pochi punti critici.

Se ne ricorderà uno brevemente. Potrebbe a prima vista apparire bizzarra l'idea del matematico inglese del Seicento John Wallis di considerare i numeri negativi *plus quam infiniti*. Eppure il suo argomento non manca di una certa plausibilità: i numeri razionali

(1) $$\ldots \frac{1}{3}, \frac{1}{2}, \frac{1}{1}, \frac{1}{0}$$

costituiscono una successione crescente. Per ogni numero naturale m, zero *escluso*, si ha infatti:

(2) $$\frac{1}{m} < \frac{1}{(m-1)}.$$

Estendendo la (2) al caso $m = 0$ si avrebbe

(3) $$\frac{1}{0} < \frac{1}{-1}$$

e ponendo, com'era relativamente abituale all'epoca (cfr. l'articolo «Zero», §§ 3.4 e 5.3), $1/0 =$ *infinito* si ottiene infinito < -1.

Naturalmente è possibile chiudere la questione dichiarando l'espressione 1/0 priva di significato. Ma si supponga invece di non rappresentare piú gli elementi di **Z** sull'usuale *retta* numerica ponendo convenzionalmente a destra dello zero i positivi e a sinistra i negativi, bensí d'impiegare la *circonferenza* numerica, secondo una proiezione centrale, come indicato nella figura 1. Il centro di proiezione K è l'unico punto della circonferenza che non ha un'immagine sulla retta: ma, come diceva il positivista logico Friedrich Waismann nella sua ormai classica *Introduzione al pensiero matematico* (*Einführung in das mathematische Denken*, 1936), «i matematici hanno l'abitudine, ogniqualvolta incontrano delle eccezioni, di formulare le cose in modo da liberarsi di esse». È immediato constatare, dalla figura 1, che se un punto si allontana sempre piú sulla retta numerica, il suo corrispondente sulla circonferenza si avvicina sempre piú a K: sulla base di tale constatazione, si può convenire che K rappresenti *il* «numero» *infinito*. Con il che l'intuizione di Wallis è riabilitata.

Dunque, non si offre sempre un *unico* modo per *ampliare* un dominio numerico. Quando si passa da un dominio numerico a uno piú ampio, il prezzo da pagare è la rinunzia a qualche «proprietà formale», cioè a qualche *regola di calcolo*, che pure valeva nel dominio di partenza; inoltre può capitare che si presentino

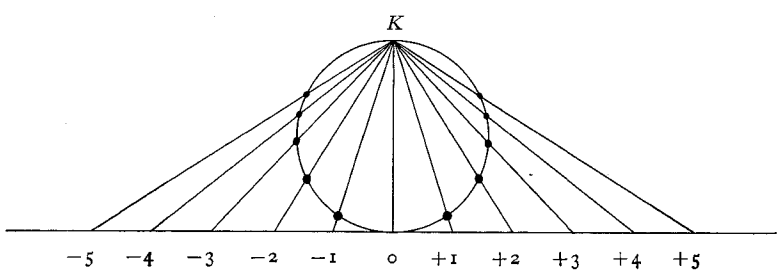


Figura 1.
La rappresentazione dei numeri relativi sulla circonferenza e sulla retta.

vie differenti, ciascuna delle quali esige la rinunzia a una *diversa* regola di calcolo. Cosí nel caso piú sopra riportato, o si vuol mantenere la formula

(4) $m > m - 1$

per $m = 0$, e in tal caso bisogna sacrificare la (2), oppure si preferisce ampliare il dominio numerico mantenendo la (2) e allora bisogna rinunziare alla (4).

Queste «biforcazioni» bene si prestano a chiarire il gioco tra la «libera» invenzione e i vincoli che sono via via posti dalle conquiste matematiche precedenti. Nell'interpretare le varie vicende essenzialisti e nominalisti sono stati spesso ciechi rispetto al nucleo razionale degli argomenti degli uni e degli altri. Nell'attuale ripresa di una concezione «fallibilista» della matematica (per esempio Lakatos, che ne ha sottolineato invece il carattere «quasi empirico», Kline, Davis e Hersch, ecc.) la «falsificazione» avviene mediante l'introduzione di nuove entità, assimilate, *via* tensione di concetto, a entità piú familiari (come alcuni «fallibilisti», in particolare Lakatos, hanno enfatizzato); viceversa, la costituzione di nuove ontologie matematiche può comportare «decisioni» concernenti la rinunzia a certe proprietà piuttosto che ad altre.

2.3. La formula risolutiva dell'equazione di terzo grado e i numeri «immaginari».

Il primo punto di riferimento restano i problemi matematici. Un *nuovo* problema può essere individuato proprio entro quel tipo di procedura che ha permesso di risolvere con successo il problema di partenza. C'è una bella metafora nel commento alla *Regula tertia decima* delle cartesiane *Regulae ad directionem ingenii*. Una statua rappresenta Tantalo, che invano accosta le labbra a un vaso colmo d'acqua per dissetarsi. «In questo vaso invero l'acqua versatavi era contenuta benissimo, fino a che non era abbastanza alta per giungere alla bocca di Tantalo; ma non appena giungeva alle infelici labbra, subito tutta scorreva via: sembra dunque, di primo acchito, che tutto l'artificio fosse riposto nella costruzione di tale statua di Tantalo, mentre in realtà questa non dà per nulla luogo alla questione, bensí l'accompagna soltanto. Tutta la difficoltà risiede infatti esclusivamente in questo e cioè nel ricercare come si possa costruire un vaso in maniera che l'acqua scorra via da esso interamente, non appena sia giunta ad una certa altezza, e prima invece in nessun modo».

Si esaminerà ora un caso per piú versi esemplare. Il problema originario è quello della soluzione per radicali dell'equazione generale di terzo grado, problema affrontato con successo dagli algebristi italiani del Cinquecento, segnatamente da Gerolamo Cardano e da Niccolò Tartaglia. Com'è noto, la procedura di Cardano e Tartaglia (per la priorità si svolse, tra l'altro, una celebre e drammatica controversia) rappresentò, agli occhi degli stessi matematici dell'epoca, il maggior contributo all'algebra successivo al tempo in cui, circa quattromila anni prima, i Babilonesi avevano insegnato a «completare il quadrato» per risolvere le equazioni di secondo grado. (Doveva seguire la scoperta della formula generale per la risoluzione delle equazioni di quarto grado; e una massa notevole

di risultati particolari concernenti le equazioni di grado superiore al quarto; piú di due secoli dopo, infine, doveva emergere l'impossibilità di risolvere per radicali l'equazione generale di grado superiore al quarto: teorema di Abel e Ruffini).

Tale procedura verrà ora schematizzata brevemente. Data l'equazione

(5) $x^3 + px = q,$

s'introducono due quantità U e T esprimendo x come differenza $T - U$. Posto $u = U^3$ e $t = T^3$ si richiede

(6) $t - u = q$

(7) $tu = \left(\frac{p}{3}\right)^3$

in modo che sia

(8) $x = \sqrt[3]{t} - \sqrt[3]{u} = T - U.$

In base alle note relazioni fra coefficienti e soluzioni dell'equazione di *secondo* grado, da (2) e da (3), per eliminazione si ottiene immediatamente:

(9) $$t = \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} + \frac{q}{2}$$

$$u = \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} - \frac{q}{2}.$$

In un primo tempo gli algebristi consideravano nella (9) il radicale positivo e, una volta determinati u e t, ne prendevano le radici cubiche (positive) per ottenere dalla (8) la «cosa», cioè l'incognita x.

A quell'epoca la pratica matematica si era ormai lasciata alle spalle il «trauma» degli irrazionali (cfr. quanto si dirà oltre, alle pp. 42-43), in quanto questi potevano facilmente venir approssimati da numeri razionali. Qualche perplessità destavano, come si è detto a p. 38, i numeri negativi. Sul piano del rigore, comunque, era sempre possibile *escludere* tali «mostri», dicendo, come già avevano fatto gli antichi Greci, che equazioni come $x^2 = 2$ e $x + 2 = 0$ ***non*** erano *risolubili*. Analogamente si poteva asserire che anche un'equazione come $x^2 + 1 = 0$ non era risolubile, e ciò evitava di dover parlare della ***radice quadrata di un numero negativo***. Ma con la comparsa del procedimento (5)-(9) le cose erano destinate a cambiare. Si supponga, per esempio, che l'espressione che compare sotto radice nella (9) risulti negativa, evenienza che caratterizza il caso in cui l'equazione (5) ammette tre soluzioni reali distinte (caso «irriducibile»). Può sembrare un paradosso: nell'equazione $x^3 = 15x + 4$, per esempio, mentre l'espressione per la «cosa» ricavata dalla (9) appare linguisticamente assurda (poiché $x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$ contiene la radice «sofistica» $\sqrt{-121}$) è abbastanza facile indovinare il valore reale dell'incognita ($x = 4$ è una soluzione dell'equazione).

È stato un altro grande algebrista italiano, Rafael Bombelli, ad affrontare con successo questo caso «irriducibile», sviluppando nella sua *Algebra* (prima edizione: 1572) quella che egli stesso considerava «un'idea assurda». Con equazioni come $x^3 = 15x + 4$ Bombelli procedeva infatti nel modo seguente: per prima cosa divideva per 3 il coefficiente del termine di primo grado ottenendo nel caso 5, lo elevava al cubo, ottenendo 125, e quindi lo sottraeva dal quadrato della metà del termine noto cioè da $(4:2)^2 = 4$; si trovava cosí di fronte a un numero negativo, il risultato dell'operazione $4 - 125$, cioè -121. Bombelli *accostava* allora alla radice quadrata di 121, cioè 11 (risultato di un'operazione *lecita*) la locuzione «piú di meno». Abbreviando ora quest'ultima locuzione con la lettera i (una piccola forzatura anacronistica), è allora possibile riassumere cosí l'ulteriore procedimento di Bombelli: alla metà di 4, cioè del termine noto, viene aggiunto «piú di meno 11, cioè $11i$. In altre parole si *forma* il «numero» $2 + 11i$ e di esso si considera la radice $\sqrt[3]{2+11i}$ per cui si ottiene $2 + 1i$ (il «2 piú di meno 1» di Bombelli) e analogamente si *forma* il «numero» $2 - 11i$ la cui radice cubica dà $2 - 1i$ (il «2 meno di meno 1» di Bombelli); infine sommando $2 + 1i$ e $2 - 1i$ si ricava 4, che è appunto la soluzione cercata.

Come la stessa notazione qui utilizzata suggerisce, il «piú di meno» di Bombelli corrisponde all'unità immaginaria delle attuali esposizioni e le espressioni composite che Bombelli formava accostando ai numeri tale locuzione o l'altra «meno di meno» corrispondono ai numeri *complessi*; in particolare l'ultimo passo si basa sul fatto che la somma di due numeri complessi coniugati dà sempre un numero reale.

Ecco, dunque, nuove «finzioni», gli immaginari, «anfibi tra essere e non essere» ancora per Leibniz, se non «assurdi» addirittura per il Cauchy del *Cours d'Analyse* (1821): comunque, dalle proprietà sconcertanti (per esempio, il corpo **C** dei complessi non è ordinato: cfr. per questa nozione l'articolo «Calcolo», § 2.4; come già osservava Bombelli, il «piú di meno», cioè l'unità immaginaria i, non risulta «comparabile» con alcun numero reale), giustificati in chiave geometrica (interpretazione di Argand, Gauss e Wessel) solo agli inizi dell'Ottocento (cfr. per esempio quanto detto in «Calcolo», § 3.6).

3. *«Fermati, attimo fuggente!»*

3.1. Procedure finitarie e infinitarie.

Si potrebbe proseguire ancora ricostruendo «ampliamenti» ancor piú lontani dall'idea piú familiare di ♦numero♦ (per esempio, numeri «ipercomplessi», come *quaternioni* di Hamilton e *ottetti* di Cayley) discutendo le motivazioni che hanno portato a questi nuovi «universi di calcolo». A questo punto pare però opportuno riflettere sulla nozione comune implicita in tutti i procedimenti computazionali presi via via in considerazione. Tale nozione è quella di ♦algoritmo♦. Intuitivamente: si tratta di un insieme finito di istruzioni per operare su simboli in modo tale da ottenere in un numero finito di passi una risposta a ogni problema di una data classe. Il termine proviene dal nome del matematico arabo al-Khuwārizmī, vissuto verso l'850, il «philosopho Algo» dei trattati di calcolo medievali, i cui lavori di *algebra* e di *aritmetica* vennero tradotti in latino nel secolo XII. È proprio in questi due campi – contrapposti alla *geometria* – che ha infatti origine una pratica di soluzione di problemi mediante la manipolazione di simboli.

Sono algoritmi, in particolare, tutte quelle procedure che constano di un numero *finito* di operazioni elementari: esse, tra l'altro, non fanno «uscire» dal corpo **Q** dei razionali. Ma i fenomeni piú diversi si possono verificare se si passa a procedure che constano di una successione *infinita* di operazioni elementari. Le procedure per l'estrazione di radice sono appunto di questo tipo: esse, in generale, fanno uscire dal dominio **Q** dei razionali, come già sapevano i Greci. La scoperta che «entità come $\sqrt{2}$ non appartengono a **Q**» (uno dei partiti piú estremi della cultura matematica greca li considerava addirittura «fuori dei numeri») rappresentò del resto una vera e propria crisi per la concezione – a un tempo matematica e cosmologica – dei pitagorici e segnò una cesura tra aritmetica e geometria, non sanata nemmeno con la rifondazione della teoria delle proporzioni dovuta ad Eudosso (e pervenutaci nel quinto libro degli *Elementi* di Euclide) che, pur risultando applicabile anche a grandezze *tra loro incommensurabili*, non aveva a che fare direttamente con «numeri», ma piuttosto con «grandezze».

Per una ricostruzione «aritmetica» (ma meglio sarebbe dire «aritmetico-insiemistica») del continuo geometrico soddisfacente i tradizionali standard di rigore occorre attendere fino alla seconda metà dell'Ottocento (costruzione di **R** a partire da **Q** secondo i metodi di Weierstrass, Dedekind, Cantor, Méray, ecc.). Ma molto prima, grazie a una tradizione calcolistica che affonda le sue radici in culture pregreche, che la «crisi degli irrazionali» non aveva del tutto spento e che si era rinnovata al contatto con le matematiche degli Indiani e degli Arabi, gli esperti dell'«arte», da Chuquet a Cardano, da Bombelli a Cataldi, ecc. sapevano «calcolare» numeri «sordi» (da «assurdi», cioè irrazionali) nei gradi di ♦approssimazione♦ voluta. La grande rivoluzione scientifica del Seicento sarebbe del resto incomprensibile se non si tenesse conto, per dirla con l'efficace frase di Koyré, della transizione dal «mondo del pressappoco all'universo della precisione». Quando, tra i tanti, un Bombelli nell'*Algebra* esalta le procedure che permettono di approssimare radici «imperfette» (cioè irrazionali) «come l'homo vorrà», realizza implicitamente entro la propria pratica scientifica l'intuizione – assai potente in quell'epoca – che la crescita della conoscenza è un processo *senza termine* cui contribuiscono, una dopo l'altra, le generazioni degli studiosi e in cui ogni passo rappresenta un progresso, seppur piccolo, rispetto alle conquiste precedenti. In questa concezione lavorare per approssimazione significa anzitutto valutazione critica degli errori: un aspetto destinato a rivelarsi sempre piú importante, col dispiegarsi dei vari tipi di calcolo e il potenziamento dei mezzi tecnologici messi a disposizione.

3.2. Il calcolo delle «flussioni» e quello dei «differenziali».

Ben prima che Georg Cantor o Richard Dedekind con le loro costruzioni di **R** a partire da **Q** o David Hilbert con la sua presentazione assiomatica di **R** fornissero quella che è stata detta «la pietra di base dell'edificio dell'analisi» evidenziando il ruolo di proprietà come la continuità in **R** o l'assioma di Eudosso-Archimede (cfr. su questi punti l'articolo «Calcolo», § 3.3), uno spregiudicato approccio a problemi di natura geometrica (come il calcolo delle aree e dei volumi, la determinazione delle tangenti, ecc.) o cinematica (determinazione della velocità, data la relazione tra spazio e tempo; il problema inverso; ecc.) dava origine a quella che Lazare Carnot doveva definire nelle *Réflexions* «una delle rivoluzioni piú rapide e felici» che mai si siano prodotte nella scienza. Non è questa la sede per ricostruire, neppure per grandi linee, la storia dell'analisi, la disciplina che gli Anglosassoni chiamano *the Calculus*, il calcolo per eccellenza. Vale la pena, però, di accennare a un punto fondamentale.

Facciamo un passo indietro. Nel libro XI delle *Confessiones* Agostino esclama: «Che cosa misuro, io Ti domando, o Dio mio, quando dico o approssimativamente: questo tempo è piú lungo di quello; o precisamente: questo tempo è il doppio di quello? Misuro il tempo, lo so; ma non misuro il futuro che non è ancora, non misuro il presente, che non occupa nessun intervallo, non misuro il passato che non è piú. Ma allora che cosa misuro? Forse il tempo nell'atto che passa, e non già quando è passato?» E «cogliere l'attimo fuggente», per usare la bella espressione dello storico delle matematiche Morris Kline, doveva essere, piú di un millennio dopo Agostino, il primo grande problema di Fermat e Pascal, di Newton e di Leibniz.

Si supponga di compiere in automobile un tragitto di 210 chilometri in tre ore. La velocità *media*, cioè la rapidità media di variazione dello spazio in relazione al tempo, sarà di 70 chilometri all'ora. Tale numero non rappresenta necessariamente la velocità in alcun *istante* di tempo particolare durante il viaggio. Ma se a un certo istante, durante il viaggio, si guarda il tachimetro, esso indica una certa quantità, poniamo 80 chilometri all'ora. Questa è appunto la velocità *istantanea*, cioè la rapidità di variazione dello spazio nell'istante in cui si guarda il tachimetro; e non significa alcunché né per il *prima* né per il *poi*. Ma è chiaro che non è possibile ottenere una velocità istantanea come si ottiene una velocità media, perché in un istante si percorre una distanza nulla e trascorre un tempo nullo: e *dividere zero per zero* sembra non avere senso.

Per meglio rendere lo slittamento creativo dovuto ai grandi matematici del Seicento e del Settecento, è bene riprendere un noto caso fisico (cfr. quanto osservato in «Approssimazione», § 1). Il movimento di una pietra che cade viene descritto assegnandone la posizione in funzione del tempo; mentre cade la sua velocità cresce, sicché la sua velocità istantanea è essa pure funzione del tempo (Newton chiamava «fluente» la posizione e «flussione» la velocità).

Nel caso della caduta della pietra la funzione «fluente», come sappiamo da Galileo, è data dalla formula $s = 4{,}9\, t^2$ ove s è il numero dei metri percorsi e t il

numero di secondi trascorsi dal momento in cui si è fatta cadere la pietra. Si voglia ora trovare la velocità *istantanea* della pietra – di cui si possiede, per ora, la sola intuizione fisica – per esempio dopo che è trascorso un secondo. Come fare? Già Fermat (ma la notazione qui impiegata è quella di Leibniz) riteneva legittimo considerare un incremento del tempo «infinitamente piccolo» dt e il corrispondente incremento ds della distanza (anch'esso «infinitamente piccolo») e definire velocità istantanea il rapporto ds/dt. Per trovare ds, l'incremento della distanza, da $t = 1$ a $t = 1 + dt$ si calcola la posizione della pietra per $t = 1$ che è $4{,}9 \times 1^2 = 4{,}9$: e la sua posizione quando $t = 1 + dt$, posizione che è $4{,}9 \times (1 + dt)^2$. Basta ora ben poca algebra per trovare che ds è $9{,}8\, dt + 4{,}9\, dt^2$. Dividendo per dt si ottiene ds/dt, la velocità istantanea, che risulta uguale a $9{,}8 + 4{,}9\, dt$. Ma poiché si cerca come risultato finale una quantità finita, si elimina il termine $4{,}9\, dt$ che, essendo il prodotto di una quantità finita per una infinitamente piccola, è a sua volta «infinitamente piccolo». Risultato finale 9,8 metri al secondo (che è il risultato corretto).

3.3. Il «principio di omissione».

È questa una tipica applicazione di un principio, il cosiddetto *principio di omissione* – apertamente teorizzato da Leibniz ma utilizzato nella pratica anche dai seguaci inglesi di Newton e da Newton stesso – che consente appunto di «tralasciare» nel risultato finale le quantità infinitesime: un principio che doveva svolgere un ruolo essenziale nella manipolazione dei «differenziali di ordine superiore». Esso è incorporato, addirittura, tra gli «assiomi» del nuovo calcolo nella *Analyse des infiniment petits* di Guillaume-François-Antoine, Marquis de l'Hôpital, il primo (1696) trattato di «analisi infinitesimale»: tali assiomi hanno appunto il compito di riportare al *discreto* di una successione di sequenze di simboli l'intuizione originaria del *continuo* che sottostà al nuovo calcolo. Ridurre a comodi algoritmi le procedure impiegate nello studio delle aree e dei volumi o nel problema delle tangenti, ecc. era del resto per Leibniz, promotore del nuovo calcolo sul continente europeo, proprio una particolare realizzazione del suo matematismo universale (cfr. p. 36).

Differente (e piú vincolata alla tradizionale intuizione geometrica e cinematica) era la giustificazione del nuovo ◆calcolo◆ offerta da Newton e dai matematici che in Gran Bretagna a lui facevano riferimento. Ma, prescindendo da questa origine bifida della nuova analisi, il vescovo Berkeley sferrava un duro attacco contro entrambi gli approcci nel suo *The Analyst* (1734), sostenendo che la matematica dei «differenziali» o delle «flussioni» era piú «oscura, precaria e ripugnante» di qualsiasi punto controverso della teologia. A parte le motivazioni apologetiche, Berkeley ragionava pressappoco cosí: dt o è uguale a zero oppure non lo è. Se dt è diverso da zero, allora anche $9{,}8 + 4{,}9\, dt$ è diverso da 9,8; se dt è zero, allora anche ds è zero, e la frazione ds/dt si riduce a un'espressione priva di significato, *zero diviso zero*. «Io ammetto, – osservava Berkeley, – che si possano inventare dei segni per denotare o qualche cosa oppure niente»; ma restava «un sofisma manifesto» conferire «un doppio significato» a simboli come dt nel

calcolo piú sopra esaminato. Berkeley veniva cosí a enunciare – con esemplare chiarezza – quelli che sono i vincoli che il rigore impone alla libertà del matematico. Vincoli che non dovrebbero venir violati: altrimenti cosa distinguerebbe la «scienza» dei matematici da una qualsiasi costruzione dell'immaginazione? (È difficile non farsi convincere, almeno per un istante, dal sarcasmo del Vescovo: «Il grande autore del metodo delle flussioni... usò le flussioni come l'intelaiatura di un edificio, come cosa da essere rimossa, non appena sono state trovate linee ad esse proporzionali. Eppure tali termini finiti sono stati trovati mediante le flussioni... E che cosa sono queste flussioni? Le velocità di incrementi evanescenti. E che cosa sono questi incrementi evanescenti? Essi non sono quantità finite, non sono infinitesimi, non sono niente. Ed allora dobbiamo forse chiamarli gli spettri di quantità morte?»).

Eppure i matematici persistettero nell'impiego di quantità «infinitesimali» ancora per un secolo, e con grande successo. Solo la reinterpretazione del calcolo infinitesimale in termini di limiti (con Cauchy) e la sua rigorizzazione (soprattutto con Weierstrass, creatore di quello «stile ε-δ» che si ritrova oggi nei vari trattati sul calcolo) dovevano relegare le quantità infinitesimali nel «pantheon degli dèi falsi e bugiardi» come si è espresso piú di uno storico della matematica. Ma qualcuno ha anche sostenuto che gli antichi dèi sono stati riabilitati – e con pregevoli risultati euristici – nell'«analisi non-standard» sviluppata negli anni '60 dal logico Abraham Robinson: Robinson ha introdotto infatti una struttura ***R** – che è indistinguibile formalmente dalla struttura **R** dei reali «standard», ma in cui **R** può venir canonicamente immersa – in cui vi sono «numeri» *infiniti* e *infinitesimi* relativamente a ogni reale standard.

(Se una morale da tale storia può essere tratta è forse questa. Per usare le parole di un filosofo della scienza – Dudley Shapere –, particolarmente interessato al fenomeno della *scoperta* scientifica: «A dispetto dei continui rimbrotti dei filosofi *à la* Berkeley, nell'impresa scientifica si sono impiegate con successo tecniche ed idee nonostante il fatto che, cosí come erano presentate, erano contraddittorie: il calcolo infinitesimale fino a Cauchy e a Weierstrass, o, da un altro punto di vista, fino a Robinson; la *funzone delta* di Dirac prima di Schwartz; e ancora certe tecniche di idealizzazione. Benché siamo stati addestrati a preferire la coerenza alla incoerenza... non c'è garanzia *a priori* che troveremo infine una reinterpretazione non contraddittoria delle nostre tecniche e idee, contraddittorie ma assai praticabili»).

3.4. Calcolo delle differenze; «legge» di continuità.

Per chiudere questo breve accenno alla «rivoluzione» nel calcolo rappresentata dalla «nuova analisi», si fisserà l'attenzione su due aspetti, entrambi fortemente presenti nell'euristica di Leibniz.

Si pensi per un momento all'oggi: gli attuali orologi digitali – piú in generale i computer ultrarapidi – rappresentano una concezione del tempo antitetica a quella tradizionale che – pur con tutte le possibili differenze, da Aristotele a Newton, da Leibniz a Weierstrass fino a larga parte della matematica e della fi-

sica del Novecento – considerava il tempo come qualcosa di *continuo*, qualcosa che ininterrottamente *fluisce*. Il tempo (come altre variabili) di un modello elaborato da un computer invece è *discreto*: al contrario che per Aristotele, qui «la natura» *fa salti*. Sarà allora istruttivo osservare che la stessa procedura infinitesimale descritta (cfr. pp. 44-45) a proposito della caduta della pietra potrebbe venir interpretata come una procedura «discreta». Basterebbe considerare *dt* come un «atomo di tempo», non ulteriormente suddivisibile per ragioni fisiche, senza però ridurlo a un istante: *dt* non si riferirebbe piú all'intervallo tra due istanti «infinitamente vicini», ma all'intervallo (finito) tra due istanti *distinti*. Il calcolo delle velocità istantanee verrebbe allora sostituito da un calcolo *approssimato* delle velocità *medie* che, dal punto di vista concettuale, è sí diverso da quello delle velocità istantanee (ed è esente dalle obiezioni di Berkeley), ma che, purché si possa prendere *dt* abbastanza piccolo, è *fisicamente equivalente* a quello delle velocità istantanee. Ciò che qui ha apportato l'«era digitale» è un potenziamento *senza precedenti* proprio del ♦calcolo♦ approssimato, sí da rendere praticabile *in tempi molto brevi* l'approccio «discreto» a problemi tradizionalmente abbordati con l'approccio «continuo». Ma i creatori del calcolo – e segnatamente coloro che, come Leibniz, miravano espressamente all'«*algebrizzazione* progressiva dell'analisi infinitesimale, cioè alla sua riduzione a un *calcolo operazionale* munito di un sistema di notazione uniforme di carattere algebrico» (per dirla con Bourbaki) – avevano già al loro tempo realizzato come un *calcolo delle differenze finite* potesse rivelarsi euristicamente utile in quanto il loro calcolo *differenziale* poteva venire ottenuto da questo mediante un passaggio al limite che – osserva ancora Bourbaki – difficilmente «si sarebbe potuto giustificare in modo rigoroso». Questo doppio modo di pensare è oggi un elemento fondamentale del calcolo (in non pochi settori: equazioni differenziali ordinarie e sistemi dinamici, equazioni alle derivate parziali, calcolo delle variazioni, ecc.) e le giustificazioni «rigorose» vengono cercate via via nel contesto dell'analisi funzionale.

La seconda questione si lega per un verso a quanto si è detto poche righe piú sopra, poiché riguarda la convinzione, espressa frequentemente da Leibniz e da alcuni dei suoi continuatori, che «i principî» della nuova analisi si applicano con successo «tanto al finito, quanto all'infinito». Come s'è detto, la giustificazione rigorosa in termini di «passaggio al limite» non era possibile in quel contesto: ciò non toglie che Leibniz ne offrisse comunque una giustificazione, anche se di tipo metafisico. Infatti: gli infinitesimi – forse piú che i numeri negativi o gli immaginari – sono non solo finzioni «utili», ma soprattutto «finzioni ben fondate», ammesse in virtú di un principio, la *loi de continuité* (quel che è vero fino al limite, è vero anche per il limite), che ne giustifica il reiterato impiego. Negli *Essais de Théodicée* (1710) Leibniz ne fornisce un interessante chiarimento: «In virtú di questa stessa legge, consegue che è possibile considerare la quiete come un movimento che scompare dopo essere stato diminuito con continuità; allo stesso modo l'uguaglianza come una disuguaglianza che essa pure scompare, come accadrebbe se si diminuisse in modo continuo il maggiore di due corpi disuguali, mentre il minore resta costante; da questa considerazione consegue che la regola generale dei corpi disuguali o dei corpi in movimento è applicabile ai corpi u-

guali, o ai corpi di cui l'uno è in quiete, come a un caso particolare della regola».

Questa metafisica *loi de continuité* di Leibniz contiene in nuce il principio di piú di una rivoluzione scientifica. Come osservava Simone Weil, dall'esterno delle matematiche, nei suoi *Cahiers* (pubblicati postumi nel 1951), intendere l'uguale come caso particolare dell'ineguale e, piú in generale, «considerare il normale come *caso particolare* dell'anormale (cosí anche il conscio come caso particolare dell'inconscio) comporta lo stesso rovesciamento che il considerare i numeri naturali come un caso particolare dei numeri complessi, o l'energia meccanica come un caso particolare dell'energia elettrica».

4. *Le macchine «inquietanti e profetiche».*

4.1. Algoritmi e macchine di Turing.

Ci si collocherà ora a un altro livello di astrazione. 1934-36: cinque logici – Gödel, Church, Turing, Post e Kleene – propongono in forma parzialmente indipendente altrettante definizioni rigorose della nozione sottostante ai processi computazionali, quella di ♦algoritmo♦ appunto. Ma perché non accontentarsi della caratterizzazione intuitiva (cfr. qui, p. 43)?

Tra le molte ragioni una permetterà di riprendere la tematica implicita nelle parole di Hobbes e di Leibniz con cui si è iniziato. Ludwig Wittgenstein, nel suo *Tractatus*, aveva affermato perentoriamente: «L'enigma non v'è. Se una domanda può porsi, *può* pure avere risposta». Si trattava di una formulazione della convinzione – che il neopositivismo contribuirà a rafforzare nella comunità scientifica – secondo cui ogni genuino problema scientifico può essere risolto applicando una procedura generale di carattere meccanico. Molti secoli prima, una convinzione di questo tipo aveva guidato gli sforzi di Lullo e dello stesso Leibniz (cfr. p. 35) verso la costruzione di un «calcolo universale» capace di generare tutte le possibili verità e di risolvere quindi tutti i possibili problemi. Inutile dire che tali sforzi erano falliti. Ma intanto un'idea estremamente feconda era venuta alla luce. Possono infatti essere viste come realizzazioni parziali del «sogno» di Lullo e di Leibniz i molti problemi che dal Seicento in avanti i matematici riuscirono a ridurre in forma algoritmica (cfr. del resto quanto osservato per l'analisi alle pp. 45-47). Nella stessa direzione si erano mosse anche le prime ricerche sulle macchine calcolatrici. Dalla macchina «aritmetica» di Pascal fino alla macchina «analitica» di Babbage, verso la metà dell'Ottocento. Di piú, in questo stesso periodo di tempo, il matematico George Boole riusciva a mostrare la natura algoritmica di alcune importanti operazioni *logiche*, estendendo cosí la nozione di calcolo dal suo tradizionale campo di applicazione quantitativo a quello *qualitativo*. E allo sviluppo di calcoli «qualitativi» sempre piú potenti e generali lavorarono a cavallo tra Ottocento e Novecento prima Gottlob Frege, poi Russell e Whitehead, e, sia pure in un'ottica diversa, il grande matematico tedesco David Hilbert. «In matematica non si dànno *Ignorabimus*», scriveva quest'ultimo nel presentare al Congresso dei matematici del 1900 una lista di ventitré problemi matematici ancora aperti. Le cose non andarono esattamente nel senso previsto. Nel 1931 Gödel dimostrava che nessuna meccanizzazione della nozione di verità aritmetica poteva essere in grado di generare tutte le verità aritmetiche; questo risultato implicava dunque l'esistenza di problemi aritmetici *insolubili in linea di principio*. La convinzione – «ragionevole» nelle parole stesse di Gödel – secondo cui ogni problema matematico poteva essere risolto meccanicamente si rivelava falsa.

Si apriva cosí alla ricerca la possibilità di affrontare i vari problemi matematici non piú tentando di costruire un ♦algoritmo♦, bensí cercando di dimostrarne la non-esistenza. Ma i risultati di questo genere *imponevano* l'uso di una *definizione rigorosa della nozione di algoritmo*. È in questo contesto che vede la luce nel 1937 il fondamentale articolo di Turing *On computable numbers, with an application to the Entscheidungsproblem* che, nelle parole di Gödel, «dà una definizione precisa, completamente adeguata e generale della nozione di procedura meccanica».

Tale definizione era formulata *via* la nozione di *macchina di Turing*. Una macchina di Turing (cfr. fig. 2) pretende di rappresentare la forma piú generale possibile di calcolatore numerico, mira cioè a conservare degli usuali calcolatori numerici soltanto le caratteristiche essenziali da un punto di vista concettuale, facendo completamente astrazione dai dettagli della realizzazione pratica. È costituita da una scorta indefinita di carta organizzata sotto forma di un nastro rettangolare suddiviso in quadratini, da un organo di «governo», e da un meccanismo di lettura-scrittura che in ogni dato istante esamina un particolare quadratino del nastro. Tali quadratini possono essere vuoti o marcati con i simboli «1». D'altra parte, l'organo di governo può trovarsi in uno tra un certo numero *finito* di stati, che possono essere pensati come configurazioni diverse di un sistema di ruote dentate oppure come diversi livelli di voltaggio. Dato il contenuto del qua-

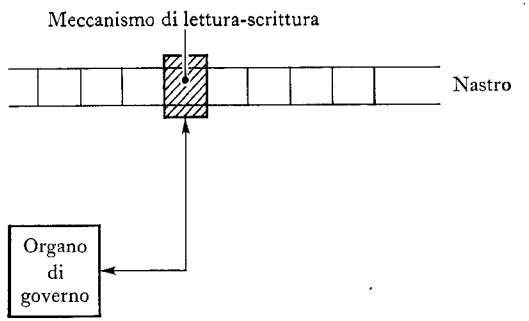


Figura 2.

Il modello fisico di una macchina di Turing. La sua struttura è estremamente semplice, come pure lo sono le operazioni elementari che è in grado di svolgere. Eppure è in grado di risolvere qualunque problema matematico per cui si disponga di un «algoritmo», cioè di una procedura meccanica di soluzione.

dratino esaminato dal meccanismo di lettura-scrittura, e lo stato dell'organo di governo, quest'ultimo può cambiare stato e impartire al primo o nessuna istruzione, nel qual caso la macchina si arresta, oppure una delle seguenti quattro istruzioni: spostarsi un quadratino a destra, spostarsi un quadratino a sinistra, scrivere il simbolo « 1 » sul quadratino esaminato (qualunque sia il suo contenuto) e infine cancellare il suo contenuto (qualunque esso sia).

Il funzionamento di una particolare macchina sarà allora completamente determinato da un programma consistente in un insieme finito di istruzioni, ciascuna delle quali specificherà – dato lo stato dell'organo di governo e il contenuto del quadratino esaminato dal meccanismo di lettura-scrittura in un dato istante di tempo – lo stato successivo del primo e quale delle quattro operazioni deve eseguire il secondo.

4.2. Risultati di impossibilità.

Tutto qui, concettualmente. Nulla di piú banale, sembrerebbe. Alla luce di quest'analisi, non possono che sembrare stravaganti le visioni apocalittiche di Samuel Butler in *Erewhon* (1872) in cui si racconta di una sanguinosa rivolta contro le macchine onde evitare che esse prendano il sopravvento sull'uomo. Tuttavia, c'è chi – come Claude Shannon, il creatore della teoria dell'informazione – le ha descritte come «inquietanti e profetiche». Perché? La ragione di fondo è che – nonostante il carattere elementare delle operazioni di cui è capace una macchina di Turing e la semplicità della sua struttura – ***non*** siamo a conoscenza di ***alcun*** algoritmo (in senso intuitivo) la cui esecuzione non sia programmabile su una macchina di Turing. La tesi che avanzò allora Turing (nota soprattutto come *tesi di Church*) è addirittura che dato un ***qualunque*** algoritmo (in senso intuitivo) esista una particolare macchina di Turing in grado di eseguirlo. Di piú egli dimostrò che, se questo è vero, allora esiste un'unica macchina di Turing (detta *universale*) in grado di eseguire qualunque algoritmo, in grado cioè di «simulare» il comportamento di ogni particolare macchina di Turing. Teorema questo che è all'origine delle ricerche di John von Neumann sulle macchine che si «autoriproducono». Un'ulteriore evidenza a favore della sua tesi la produsse lo stesso Turing dimostrando l'equivalenza tra la sua definizione e quella di Church. Non solo, ma tutte le definizioni alternative si rivelarono equivalenti alla prima. La superiorità della definizione di Turing consisteva essenzialmente nel fatto che approssimava il modo in cui effettivamente si svolgono i processi computazionali, sembrava anzi cogliere le loro caratteristiche essenziali.

Tanto piú sorprendenti allora i risultati di *insolubilità* ottenuti dallo stesso Turing e da molti altri. Tra questi, forse il piú interessante matematicamente è quello concernente l'insolubilità del *decimo problema* di Hilbert: costruire un algoritmo che determini se una certa classe di equazioni (dette *diofantine*) ammette o meno una soluzione in numeri interi relativi. Il piú interessante filosoficamente è quello concernente l'insolubilità del cosiddetto problema della *decisione* (ottenuto dallo stesso Turing): costruire un algoritmo che determini se una arbitraria formula appartenente a una certa classe di teorie matematiche (dette del *prim'ordine*) ammette o meno una dimostrazione entro di esse. Esso si rivelò equivalente a un problema molto piú importante entro la teoria degli automi: costruire un algoritmo che determini se il tempo di esecuzione di un arbitrario programma è o meno finito. Si trattava di un risultato di impossibilità che doveva svolgere entro questa teoria lo stesso ruolo di analoghi teoremi di impossibilità in matematica (si pensi al teorema di Abel-Ruffini) e in fisica (per esempio: è impossibile un *perpetuum mobile* del I tipo, è impossibile un *perpetuum mobile* del II tipo, è impossibile lanciare un segnale a una velocità maggiore della luce, ecc.). [G. G. e M. M.].

Apéry, R., e altri
1982 *Penser les mathématiques. Séminaire de philosophie et mathématiques de l'Ecole normale supérieure*, Seuil, Paris.

Apostol, T. M.
1969 *Calculus*, Wiley, New York 1969² (trad. it. Boringhieri, Torino 1977-78).

Baron, M.
1969 *The Origins of the Infinitesimal Calculus*, Pergamon Press, Oxford - New York.

Bochner, S.
1966 *The Role of Mathematics in the Rise of Science*, Princeton University Press, Princeton N.J.

Bos, H. J. M.
1974 *Differentials, higher-order differentials and the derivation in the Leibnizian calculus*, in «Archive for History of Exact Sciences», XIV, pp. 1-90.

Bottazzini, U.
1981 *Il calcolo sublime. Storia dell'analisi matematica da Euler a Weierstrass*, Boringhieri, Torino.

Bourbaki, N.
1960 *Eléments d'histoire des mathématiques*, Hermann, Paris (trad. it. Feltrinelli, Milano 1963).

Boyer, C. B.
1968 *A History of Mathematics*, Wiley, New York (trad. it. Isedi, Milano 1976).

Browder, F.
[1974] (a cura di) *Mathematical Developments Arising from Hilbert Problems. Symposium in Pure Mathematics, Northern Illinois University, 1974*, American Mathematical Society, Providence R.I. 1976.

Courant, R., e Hilbert, D.
1953-62 *Methods of Mathematical Physics*, 2 voll., Interscience and Wiley, New York - London.

Davenport, H.
1970 *The Higher Arithmetic. An Introduction to the Theory of Numbers*, Hutchinson, London 1970².

Davis, Ph. J., e Hersch, R.
1981 *Mathematical Experience*, Birkhauser, Boston.

Dieudonné, J.
1968 *Calcul infinitésimal*, Hermann, Paris.
1969 *Foundations of Modern Analysis*, Academic Press, New York.
1977 *Panorama des mathématiques pures. Le choix bourbachique*, Gauthier-Villars, Paris.
1981 *History of Functional Analysis*, North-Holland, Amsterdam.

Dieudonné, J., e altri
1978 *Abrégé d'histoire des mathématiques (1700-1900)*, Hermann, Paris.

Dugac, P.
1973 *Eléments d'analyse de K. Weierstrass*, in «Archive for History of Exact Sciences», X, pp. 40-176.

Edwards, C. H.
1980 *The Historical Developments of the Calculus*, Springer, Berlin - Heidelberg - New York.

Feigenbaum, E. A., e Feldman, J.
1963 (a cura di) *Computers and Thought*, McGraw-Hill, New York.

Félix, L.
1957 *L'aspect moderne des mathématiques*, Blanchard, Paris.

Goldstine, H. H.
1972 *The Computer from Pascal to von Neumann*, Princeton University Press, Princeton N.J.
1977 *A History of Numerical Analysis. From the 16th through the 19th Century*, Springer, Berlin - Heidelberg - New York.
1980 *A History of the Calculus of Variations from the 17th through the 19th Century*, Springer, Berlin - Heidelberg - New York.

Grabiner, J. V.
1981 *The Origins of Cauchy's Rigorous Calculus*, Mit Press, Cambridge Mass.

Grattan-Guinness, I.
1970 *The Development of the Foundation of Mathematical Analysis from Euler to Riemann*, Mit Press, Cambridge Mass.
1980 (a cura di) *From Calculus to Set Theory. An Introductory History*, Duckworth, London.

Hawkins, Th.
1970 *Lebesgue's Theory of Integration. Its Origins and Development*, University of Wisconsin Press, Madison Wis.

Ifrah, G.
1981 *Histoire universelle des chiffres*, Seghers, Paris.

Kline, M.
1972 *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York.
1980 *Mathematics. The Loss of Certainty*, Oxford University Press, New York.

Knuth, D. E.
1965 *The Art of Computer Programming*, I. *Fundamental Algorithms*, Addison-Wesley, Reading Mass.
1969 *The Art of Computer Programming*, II. *Seminumerical Algorithms*, Addison-Wesley, Reading Mass.

Lakatos, I.
[1961-74] *Proofs and Refutations. The Logic of Mathematical Discovery*, Cambridge University Press, London 1976 (trad. it. Feltrinelli, Milano 1979).

Le Lionnais, F.
1948 (a cura di) *Les grands courants de la pensée mathématique*, Cahiers du Sud, Marseille; nuova ed. Blanchard, Paris 1962.

Minsky, M. L.
1967 *Computation, Finite and Infinite Machines*, Prentice-Hall, Englewood Cliffs N.J.

Monna, A. F.
1973 *Functional Analysis in Historical Perspectives*, Oosthoek, Utrecht.

Picutti, E.
1977 *Sul numero e la sua storia*, Feltrinelli, Milano.

Priestley, W. M.
1979 *Calculus; an Historical Approach*, Springer, Berlin - Heidelberg - New York.

Ralston, A.
1965 *First Course in Numerical Analysis*, McGraw-Hill, New York.

Randell, B.
1975 (a cura di) *The Origins of Digital Computers. Selected Papers*, Springer, Berlin - Heidelberg - New York 1975[2].

Somenzi V.
1965 (a cura di) *La filosofia degli automi*, Boringhieri, Torino.

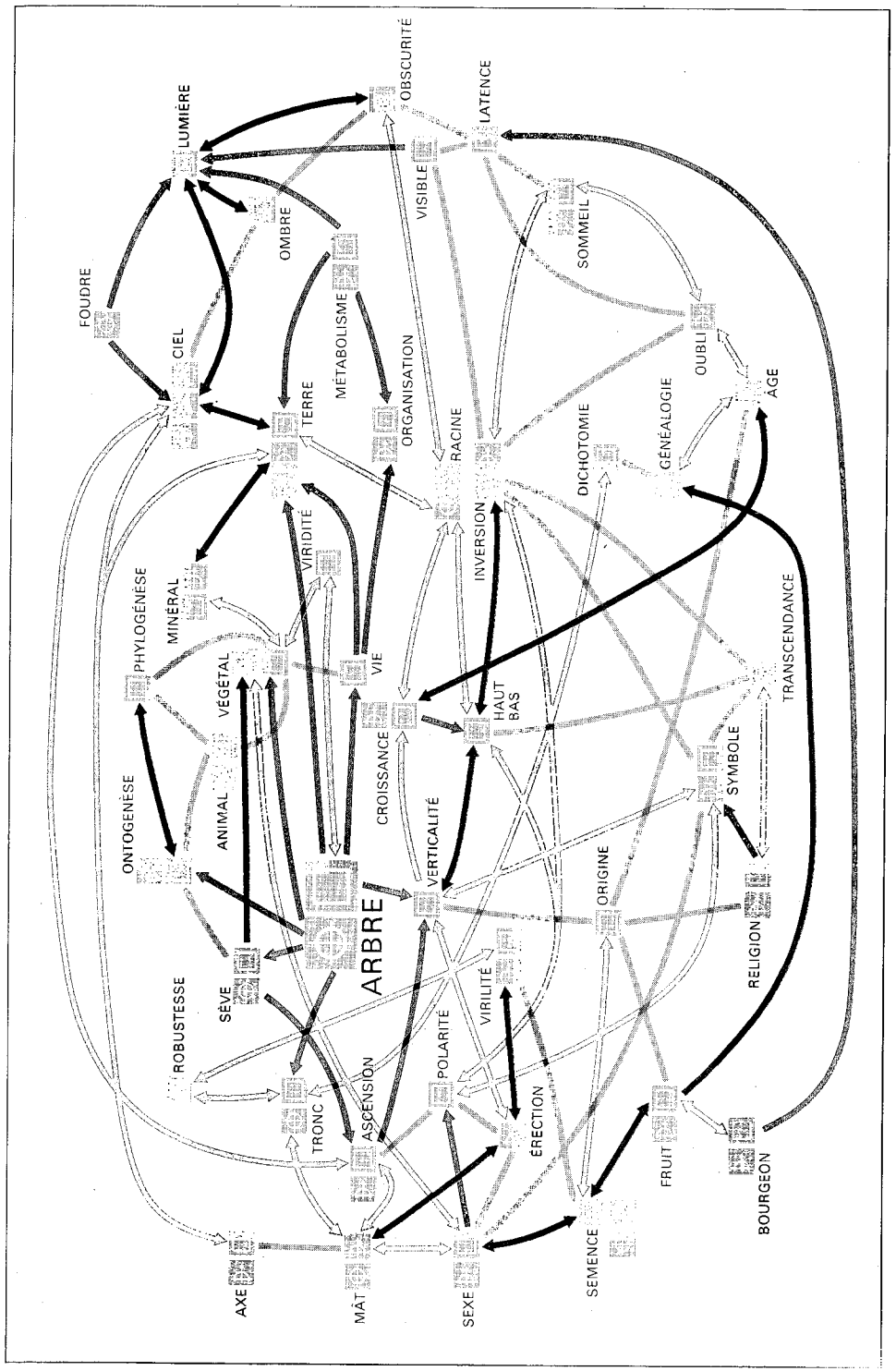
Sondheimer, E., e Rogerson, A.
1981 *Numbers and Infinity. A Historical Account of Mathematical Concepts*, Cambridge University Press, London.

Struik, D. J.
1967 *A Concise History of Mathematics*, Dover, New York 1967[3] (trad. it. Il Mulino, Bologna 1981).

Temple, G.
1981 *100 Years of Mathematics*, Duckworth, London.

Weil, A.
1973 *Basic Number Theory*, Springer, Berlin - Heidelberg - New York 1973[2].

Zellini, P.
1980 *Breve storia dell'infinito*, Adelphi, Milano.



29. *Tableau de relations*, dal XVII volume (*Organum*) dell'*Encyclopaedia Universalis* (Paris 1973).

Abaco

È caratteristica fondamentale dell'uomo l'essere in grado di costruire strumenti mediante i quali egli si pone in condizione di esercitare un'azione che va oltre le sue facoltà strettamente biologiche. L'invenzione e l'uso di tali strumenti, ossia la tecnica, riguardò dapprima le sfere d'interesse vitale delle attività meccaniche e chimiche, per poi estendersi a bisogni di tipo essenzialmente sociale. Di questi ultimi fanno parte, innanzitutto, la tecnicizzazione della comunicazione, della numerazione e del calcolo.

Il concetto di numero si forma assai tardi e, al di là di una certa quantità (dipendente del resto dal grado di sviluppo culturale), sfugge ad ogni facoltà rappresentativa: l'uomo ha cominciato dunque col servirsi di quantità ausiliarie.

Come in ogni altro ramo della tecnica, anche qui si ricorre in primo luogo a certe parti del corpo umano, in particolare alle dita: in tal modo ha origine il calcolo, origine che del resto influisce ampiamente in quasi tutte le lingue sulla determinazione dei caratteri numerali, ma comunque non consente di rappresentare agevolmente i valori piú elevati.

In secondo luogo, per ritenere una certa quantità si ricorre ad oggetti d'uso comune e d'ugual forma, come sassolini, bastoncini, grani, ecc.

In terzo luogo, l'intero sistema finisce per divenire uno strumento artificiale, quale un bastone segnato con delle tacche o un *quipu* (cordone a nodi degli Inca), oppure in forma di cifre presso i popoli che conoscono la scrittura.

Nel passaggio dalla seconda alla terza fase si compie un processo mentale, premessa di tutti i metodi di calcolo successivi: mediante aggruppamento di piú unità la serie numerica diviene prontamente afferrabile. L'aggruppamento di 5, 10 o 12 unità in un'unità d'ordine superiore avviene presso tutti i popoli prima ancora che la lingua abbia avuto modo di formare l'intera serie dei numerali. Per questo anche nelle lingue piú evolute si possono ravvisare tracce degli aggruppamenti primitivi: si consideri ad esempio il greco πεμπάζειν 'contare per cinque' (e generalmente 'calcolare') o il francese *quatre-vingt* 'ottanta' (letteralmente 'quattro volte venti').

Le unità dei vari ordini, che includono ordini di numeri in successione ascendente, si formano spontaneamente, e il sistema che ne risulta non sempre ubbidisce alla logica matematica. Cosí la numerazione sessagesimale babilonese, pur fondandosi sulla serie esponenziale del numero 60, fa uso altresí del numero 10 come unità d'ordine secondaria. I Maya, dal canto loro, aggruppavano le unità semplici sotto il 10, quindi sotto il 20 e le potenze di quest'ultimo numero (400, 8000, 160 000). La moneta medievale si fondava su una contaminazione del sistema duodecimale con quello vigesimale.

A quantità ausiliarie ed alla suddivisione in unità d'ordine vieppiú elevato si ricorreva in quanto esse erano atte a 1) ritenere delle quantità di certi oggetti, e 2) addizionare o sottrarre. Per tutte le altre necessità, in particolare per moltiplicare e per dividere, si dovette elaborare un metodo specifico.

1. *I primordi dell'abaco.*

Come oggi, nell'insegnamento che viene impartito ai bambini, la moltiplicazione viene ricavata a partire dall'addizione, si può senz'altro ritenere che in origine gli uomini, a partire dalle stesse premesse, eseguissero empiricamente

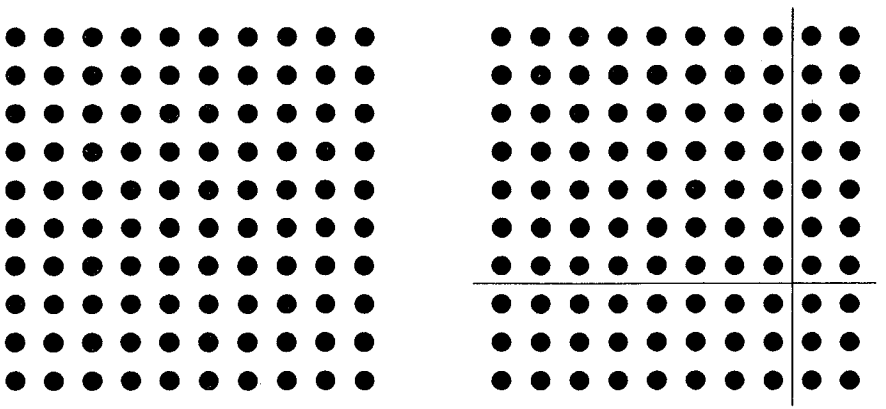
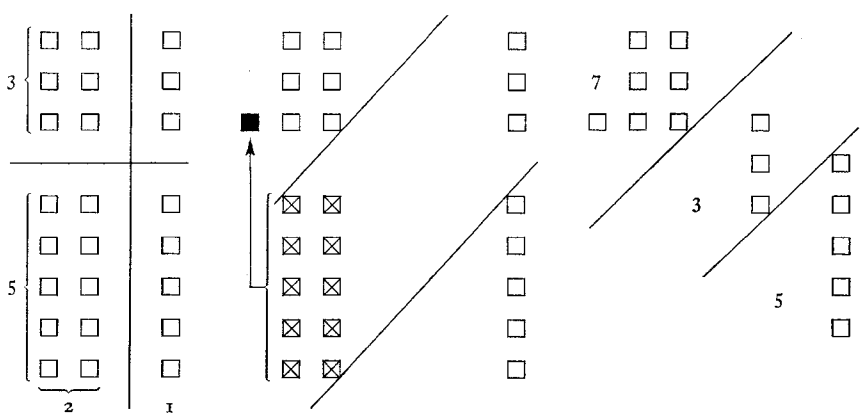


Figura 1.
Tavola per eseguire moltiplicazioni dal papiro 10184 (Salier 4), British Museum (a sinistra) ed esecuzione della moltiplicazione 7×8 secondo il sistema egiziano.



a) Disposizione dei fattori 35×21. *b*) Riordinamento. *c*) Soluzione = 735.

Figura 2.
Moltiplicazione secondo il metodo di Yu Chen-shan.

operazioni elementari di moltiplicazione. Un'altra parola greca per 'calcolare', ψηφίζειν (da ψῆφος 'sassolino', lat. *calculus*), come pure le espressioni latine corrispondenti *calculos ponere* e (nel medioevo) *calculare*, indicano l'esistenza di un metodo di calcolo primitivo che consentiva già di eseguire delle moltiplicazioni elementari.

Esso consisteva probabilmente nel trasporre il moltiplicando in tante file di pietruzze disposte l'una sotto l'altra, quante lo richiedeva il moltiplicatore: quindi le pietruzze venivano contate e il numero ottenuto messo per iscritto. Una variante di questo metodo presso gli Egiziani, che conoscevano la scrittura, è indicata da due papiri del British Museum: un quadrato formato da dieci puntini per dieci (fig. 1) era evidentemente destinato a facilitare l'esecuzione di moltiplicazioni comprese entro la tavola pitagorica; coprendo una parte del quadrato oppure tirando delle linee se ne può ricavare qualsiasi risultato, in analogia con il metodo del calcolo eseguito con le pietre.

Che questo genere di soluzioni empiriche, il cui schema fondamentale è inerente alla facoltà astrattiva dell'uomo, si ripresenti di continuo, è attestato, per esempio, dall'invenzione che un artigiano cinese fece nel 1959 (fig. 2): grazie ad essa è possibile moltiplicare tra loro numeri di piú cifre (tenendo conto, naturalmente, del sistema accettato, che in questo caso è quello decimale) per mezzo di semplici dadi oppure graficamente, senza che sia richiesta una conoscenza specifica del calcolo.

2. *Origine dell'abaco.*

Per abaco s'intende uno strumento che consente di eseguire le quattro operazioni fondamentali con numeri interi positivi e con frazioni semplici fino ad ordini di grandezza praticamente illimitati, e in cui il concetto di numerazione posizionale è inconsapevolmente anticipato, senza tuttavia ch'esso venga necessariamente applicato nella numerazione scritta.

Qui è presupposta la conoscenza della serie numerica oppure della numerazione scritta, ordinate con chiarezza mediante la loro suddivisione in unità di ordine diverso e ascendente, nonché la conoscenza e l'uso della tavola pitagorica. Bisogna ritenere che queste condizioni si verifichino necessariamente quando l'attività tecnico-amministrativa e/o commerciale raggiunge un determinato livello. Tuttavia questo livello, conseguenza dello sviluppo sociale e dell'organizzazione statale, venne raggiunto (nell'antichità e nel medioevo) indipendentemente in aree diverse di civiltà. Di conseguenza, strumenti di calcolo adeguati fecero la loro comparsa in Mesopotamia, nei paesi del Mediterraneo orientale, nell'Asia orientale, in America.

L'esistenza dell'abaco non è direttamente accertata a Babilonia, tuttavia sia il ritrovamento di tavole di moltiplicazione con quadrati fino a 743^2, risalenti al principio del II millennio a. C., sia l'impiego di una numerazione posizionale dotata di segni per i posti vuoti (quasi-zeri), d'epoca posteriore, depongono in favore della presenza e dell'uso dell'abaco.

L'esistenza di economie e di sistemi di computo assai evoluti anche nell'Egitto del Nuovo Regno ed a Creta, e le esigenze commerciali delle città fenice, fanno supporre una contemporanea presenza dell'abaco nel Mediterraneo orientale. L'abaco egiziano è tuttavia documentato soltanto nel V secolo a. C. da un passo di Erodoto [*Storie*, II, 36]: «Gli Elleni scrivono e fanno il conto portando la mano da sinistra a destra, gli Egizi da destra a sinistra».

Non vi sono dubbi, invece, circa la forma ed il modo d'impiego dell'abaco greco – prodotto senz'altro di una delle civiltà summenzionate –, il cui nome ('superficie piana, tavolo, tavola per far di conto') ed il cui uso passarono ai Romani. Una dozzina di abaci greci in marmo, nonché un gran numero di passi in autori classici ed alcune figure, ne facilitano la ricostruzione. Ci sono pervenuti anche alcuni esemplari d'abaco, piccoli e maneggevoli, d'epoca romana.

Ora, mentre tutti questi tipi di abaco, in parte ipotetici, dovrebbero avere un'origine comune, lo stesso non può dirsi dell'abaco dell'Estremo Oriente.

L'abaco cinese (*swan pan*), posto talvolta in rapporto con quello romano, benché documentato soltanto a partire dal XIII secolo, ebbe un'evoluzione altrettanto indipendente della numerazione scritta cinese, simile anch'essa ai sistemi occidentali. Ciò è dimostrato principalmente dalla piú che millenaria esistenza dei bastoncini *ciau* (in giapponese *sanghi*), che, nell'operazione di calcolo, venivano disposti su di un'asse secondo principî simili a quelli regolanti l'uso dell'abaco. Al piú presto attorno al 1600, poi, lo *swan pan* passò (con il nome di *soroban*) in Giappone, ed un po' piú tardi in Russia. Queste palline ordinate su fili o su asticelle sono cosí maneggevoli che lo *swan pan* è l'unica forma di abaco che sia sopravvissuta fino ad oggi.

Anche l'esistenza dell'abaco nell'America precolombiana è soltanto ipotetica; tuttavia è corroborata da una serie d'indizi. Innanzitutto un calendario straordinariamente raffinato, che si serviva di una numerazione scritta facente uso del valore posizionale e dello zero (presso i Maya), ed inoltre due figure di provenienza azteca ed incaica, fanno pensare che già in epoca precolombiana fosse nota una forma d'abaco simile a quella esistente nell'emisfero orientale.

Ciò non significa che non siano esistiti abaci in altre civiltà, di cui non si parlerà in questa sede: per esempio è quasi fuor di dubbio che in India, paese d'origine delle cosiddette cifre arabe, si praticò nella tarda antichità un metodo di calcolo che doveva necessariamente condurre alla loro scoperta.

3. *Il calcolo con l'abaco.*

L'abaco occidentale, la cui ininterrotta esistenza per due millenni deve considerarsi provata, servirà qui ad illustrare i tipi di calcolo piú comuni. Data l'oscurità delle prime descrizioni dell'abaco in nostro possesso, risalenti al medioevo, ci si baserà sui manuali del XVI secolo, utilizzando anche i termini tecnici in essi contenuti e desunti dalla tradizione medievale.

3.1. Numerazione.

Le unità dei vari ordini del sistema decimale sono rappresentate sull'abaco per mezzo di linee verticali (presso i Greci ed i Romani) oppure orizzontali (a partire dal medioevo). Talvolta sono utilizzati a tale scopo gli spazi compresi tra le linee (*spatium*), solitamente riservati ai valori intermedi dei numeri romani (V, L, D). La tavola viene divisa in due parti onde poter disporre gli uni accanto agli altri gli addendi o i fattori. Le unità delle migliaia vengono spesso indicate con una X.

L'atto di disporre i numeri – a mezzo di pietruzze o di gettoni – si chiamava numerazione e veniva eseguito in conformità al sistema delle cifre romane (fig. 3). Ecco perché i segni numerici romani continuarono a vivere in stretta simbiosi con l'uso dell'abaco, anche quando le cifre arabe fornirono una facile alternativa.

L'abaco, d'altra parte, dovette essere preferito anche in epoca successiva se

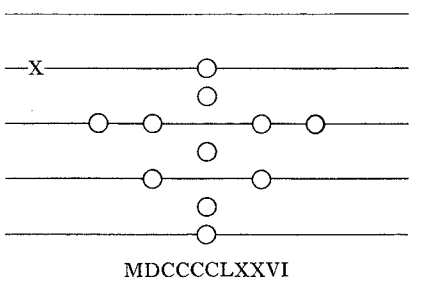


Figura 3.
Il numero 1976 rappresentato mediante gettoni disposti su linee.

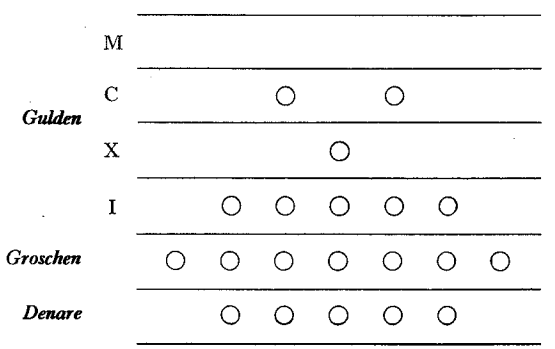


Figura 4.
215 *Gulden*, 7 *Groschen*, 5 *Denare* disposti fra le linee.

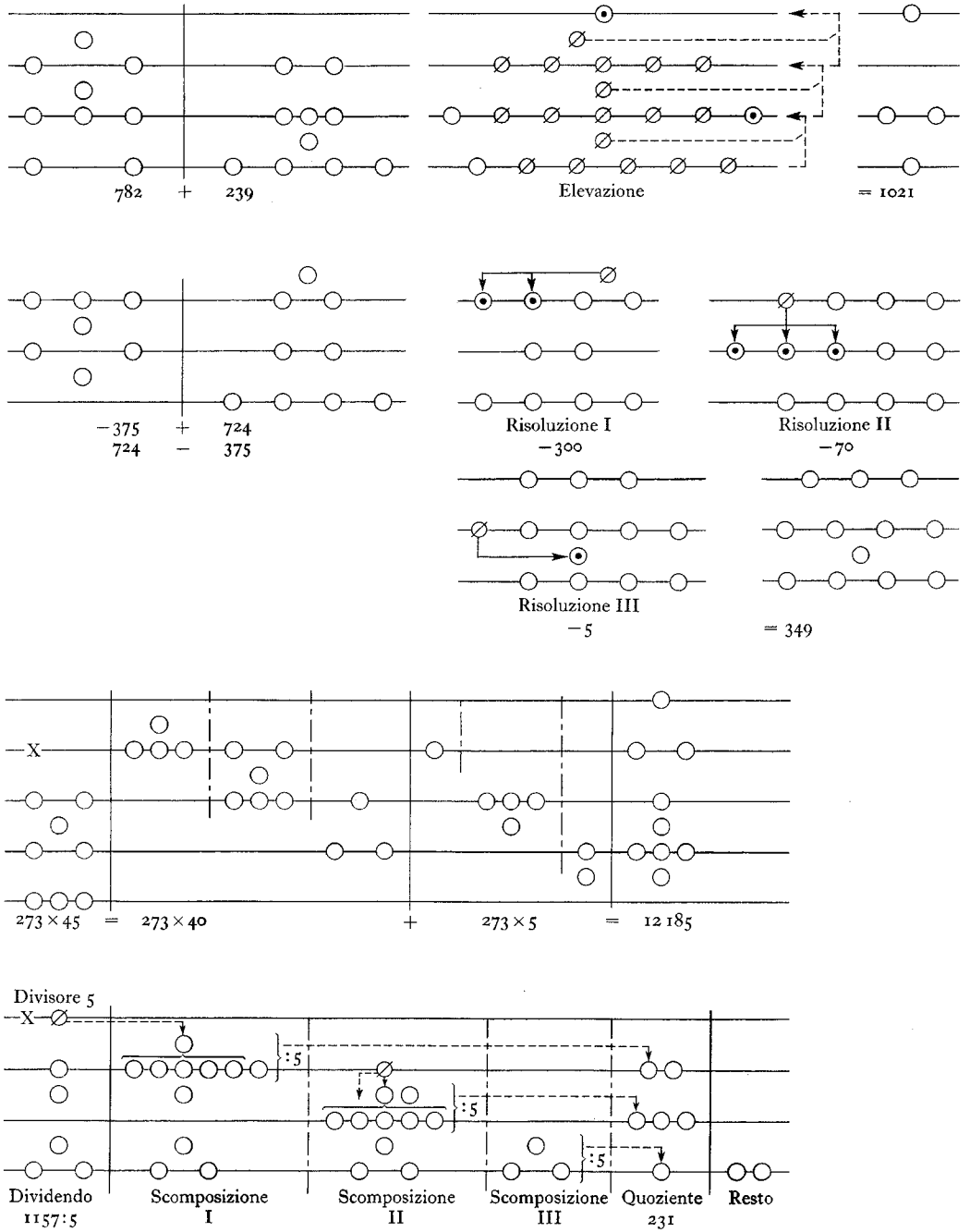


Figure 5-8.

Le quattro operazioni eseguite sull'abaco. Dall'alto in basso: addizione, sottrazione, moltiplicazione, divisione.

si trattava di eseguire calcoli sulle unità monetarie o con sistemi di misura. I vantaggi dell'abaco risultavano evidenti, per esempio, quando si trattava di far dei conti in fiorini, sapendo che un *Gulden* conteneva 21 *Groschen*, e un *Groschen* 12 *Denare* (fig. 4).

Si comprenderà allora perché la scomparsa dell'abaco dalla sua ultima roccaforte – l'amministrazione finanziaria statale francese – abbia coinciso con l'introduzione dell'ordinamento decimale nei sistemi monetario e di misura.

3.2. Addizione e sottrazione.

Dopo aver trasposto i due valori numerici l'uno accanto all'altro sull'abaco, i gettoni venivano (nel caso dell'addizione) raggruppati, contati e risolti in unità d'ordine superiore, e quindi elevati: cioè, gettoni del medesimo ordine numerico che venissero ad essere in quantità superiore a 10 (oppure a 5), venivano tolti e sostituiti da un gettone d'ordine superiore; questa operazione veniva compiuta prima sulle unità, elevandole a decine, poi sulle decine, elevandole a centinaia, e cosí via. Infine si leggeva la somma ottenuta e la si metteva per iscritto (fig. 5).

Per fare una sottrazione, il sottraendo doveva venir disposto sulla sinistra, e l'operazione era eseguita sulla parte destra dell'abaco (fig. 6). Qui si trattava, poi, non di elevare le unità inferiori ad unità superiori, bensí di risolvere le unità d'ordine superiore in unità d'ordine inferiore (risoluzione).

3.3. Moltiplicazione.

Quale fase preparatoria di questa operazione vanno indicati il raddoppiare e il dimezzare, che venivano considerati come una categoria a parte. Se per esempio si trattava di calcolare 23×64, si procedeva raddoppiando il primo numero tante volte, quante era possibile dimezzare il secondo (46×32, 92×16, ecc.), finché non si arrivava al risultato desiderato (1472×1). In presenza di numeri dispari, si operava correttivamente sui resti.

La moltiplicazione vera e propria comportava una difficoltà maggiore, soprattutto perché richiedeva la conoscenza della tavola pitagorica. A questa carenza si rimediava spesso con l'ausilio di tavole di calcolo. In questo caso, però, occorreva determinare con precisione, ad ogni passaggio, la disposizione delle unità di conto: infatti qui s'incorreva spesso in errore. La moltiplicazione cominciava sempre dai valori piú alti (fig. 7); il moltiplicatore, solitamente, non veniva segnato sulla tavola, ma – come è detto in un manuale di calcolo – «tenuto a mente, ricordato con l'aiuto delle dita oppure messo per iscritto».

3.4. Divisione.

Essendo questa operazione di gran lunga la piú difficile, i manuali di calcolo consigliano molti metodi di divisione, i quali tuttavia – soprattutto in certi casi – rischiano sempre di condurre a dei punti morti. La determinazione degli

esatti valori posizionali delle divisioni singole viene resa piú complicata dalla risoluzione delle unità d'ordine superiore, che si rende necessaria quando il dividendo è minore del divisore.

Eppure anche qui si rivelò la grande funzione didattica dell'abaco nella scoperta e nell'applicazione consapevole del principio posizionale: se, per esempio, si ha da dividere 279 per 9, i due gettoni disposti sulla linea delle centinaia devono venir risolti in 20 sulla linea delle decine, affinché sia possibile eseguire la divisione. Un semplice esempio basta ad illustrare questo principio (fig. 8).

Si sono cosí brevemente delineati i calcoli che venivano eseguiti sull'abaco europeo del tardo medioevo: o almeno quelli che bastavano a soddisfare le esigenze di un semplice mercante o d'un'amministrazione comunale. I manuali di calcolo, tuttavia, insegnavano anche a risolvere problemi piú complessi, come calcoli monetari, calcoli degli interessi e persino estrazioni di radici: assai di rado però tali calcoli venivano praticamente eseguiti.

4. *L'abaco nella vita quotidiana.*

Può sembrare ovvia l'affermazione che la scrittura costituisca una conquista dell'uomo posteriore alla conoscenza della numerazione scritta e del calcolo. Tale affermazione acquista però importanza quando si consideri che nell'antichità e nel medioevo esisteva uno strato sociale incivilito, composto di contadini, di cittadini e persino di mercanti, che doveva e sapeva far di conto pur senza essere in grado di scrivere. Nell'introduzione del *Livre des Getz* (= *des jetons*), testo francese della fine del XV secolo, è detto espressamente che «vi sono molti mercanti che non sanno né leggere né scrivere, ma devono per forza saper contare bene». L'attività commerciale, l'amministrazione di una proprietà fondiaria e persino il cambio di valuta sono concepibili anche senza la conoscenza della scrittura, ma non senza quella dell'abaco.

4.1. L'apprendimento.

L'apprendimento del calcolo fu, sin dall'antichità, legato a quello del leggere e dello scrivere. Il fanciullo romano è definito «puer litteris elementariis et calculo imbutus» [Giulio Capitolino, *Pertinax*, 1, 4]; inoltre viene esplicitamente affermato ch'egli si recava a scuola con la tavoletta per il calcolo e i sassolini [Orazio, *Satirae*, I, 6, 74]. Una caricatura d'epoca romana ci ha conservato un'immagine di vita scolastica, in cui compaiono scolari con tavoletta per scrivere ed abaco.

I maestri di calcolo romani o *calculatores* (da non confondersi con i *calculones*, che erano gli schiavi che facevano di conto) percepivano, in base alle tariffe retributive di Diocleziano, un compenso maggiore dei maestri elementari, ma tuttavia minore degli insegnanti di geometria o *arenarii*.

La documentazione riguardante il medioevo è scarsa, anche se gl'insegnanti

di calcolo sono spesso menzionati nei testi. Il Quadrivio comprendeva l'insegnamento dell'aritmetica; tuttavia gli autori, da Boezio, a Beda, a Gerberto, menzionano l'abaco solo di sfuggita.

A partire dal XV secolo, in tutte le città si trovano delle scuole di calcolo, spesso delle corporazioni, che riunivano i maestri di calcolo (nel 1613 Norimberga aveva già 48 maestri). A volte l'insegnamento era gratuito. Un documento della città di Rostock, nella Germania settentrionale, afferma infatti esplicitamente che il maestro di calcolo deve insegnare «gratuitamente a tutti i fanciulli senza distinzione... a scrivere, a far di conto e a tener la contabilità».

Grande importanza ebbero altresí i manuali di calcolo (in particolare quello del Recorde in Inghilterra, del Clichtovaeus in Francia, del Perez de Moya in Ispagna, del Riese in Germania e del Frisius in Olanda), che, apparsi soprattutto con lo scopo d'introdurre le cifre arabe, contribuirono a diffondere, a partire dall'ultimo quarto del XV secolo, l'uso dell'abaco. Uno di questi autori, Petrus Apianus, osserva nel 1527 che le monete per far di conto sono maggiormente usate del calcolo con le cifre, ed il piú famoso di essi, Adam Riese, scrive nella prefazione al suo *Rechnung auff der Linihen und Federn* (1529): «Nel corso della mia attività di ammaestramento della gioventú, ho trovato che coloro i quali principiano a calcolar sulle linee [ossia sull'abaco], finiscono sempre per diventare piú abili e piú spediti nel calcolo di quelli che cominciano con le cifre».

Questa considerazione è suffragata dall'esperienza didattica odierna, la quale, fondandosi parimenti sull'uso d'insiemi concreti, insegna agli scolari gli elementi primi del calcolo. Qui è opportuno aggiungere che il diffusissimo pallottoliere (*boulier*) usato dai bambini trae origine dall'abaco russo (*sčoty*), e ch'esso venne introdotto in Occidente dopo il 1812 dal francese Poncelet, sulla base di una sua esperienza nella regione della Volga. È cosí che ancor oggi molti scolari imparano le operazioni fondamentali sull'abaco.

4.2. Impiego dell'abaco nella sfera privata.

Un maestro di calcolo tedesco della metà del XVI secolo, Michael Stiefel, afferma non esservi «governo d'una casa, per piccolo e cattivo che sia, a cui non torni utile tenere una contabilità», e che questa viene «appresa in modo straordinariamente facile grazie alle monete per far di conto [cioè l'abaco]». Testimonianze letterarie [Giovenale, *Satirae*, IX, 40; Marziale, *Epigrammata*, II, 48, 2] provano che anche nell'antichità l'amministrazione domestica faceva uso dell'abaco: ancor meglio ciò può desumersi da un rilievo dell'età imperiale, in cui è raffigurato un moribondo nell'atto di suddividere i suoi beni tra gli eredi, con accanto un servitore che addiziona su di un abaco le somme di denaro.

Naturalmente l'uso dell'abaco è molto piú frequente presso mercanti ed usurai, dei quali già nelle lettere di Alcifrone un contadino si lamenta con queste parole: «È un tormento questa gente, che fa di conto con dei sassolini e piegando le dita» [I, 26]. Anche la prima raffigurazione pervenutaci di un panno per eseguire calcoli, che si trova in un manoscritto inglese del XIV secolo, reca la

dicitura «tavola mercantile per tutti i conti». Scrive il contemporaneo Chaucer: «dispose davanti sulla sua tavola per i conti i suoi libri e molti gettoni»...

Nelle numerose stampe dei secoli XV-XVIII, da Urs Graf fino a Hogarth, si possono veder rappresentati banchieri, commercianti e rigattieri nell'atto di eseguire calcoli sull'abaco.

Che questo stesso strumento di calcolo fosse altrettanto familiare persino al semplice contadino, può desumersi dal monologo del giovane pastore nel *Winter's Tale* di Shakespeare [IV, II], come pure dal fatto che in Ungheria quel metodo di calcolo viene espressamente designato come «calcolo del contadino».

4.3. Impiego dell'abaco nell'amministrazione.

L'amministrazione cittadina e statale non ha mai potuto fare a meno dell'abaco. Ad Atene esso veniva impiegato sia nello scrutinio delle votazioni sia nel calcolo degl'interessi.

Nel medioevo i sovrani non ritenevano lesivo della loro dignità prender parte personalmente alle operazioni contabili. Di Carlo il Temerario di Borgogna si legge: «lui stesso siede a un capo del tavolo, disponendo dei gettoni e calcolando come gli altri, e non c'è differenza tra loro in questo esercizio se non che il duca usa gettoni d'oro e gli altri d'argento».

Le monete per far di conto (i gettoni sono un'invenzione dell'amministrazione statale francese del XIII secolo) sono dapprincipio prodotte, come attività secondaria, dalle zecche, in seguito da maestri specializzati, e finalmente divengono di uso comune.

La camera dei conti della casa reale inglese si chiamava «Court of Green Cloth», perché i conti venivano eseguiti sopra dei panni verdi. Panni consimili venivano usati dall'amministrazione bavarese attorno al 1700, e ci sono stati conservati: su di un panno verde sono cucite delle cordicelle gialle, e le abbreviazioni delle unità dei vari ordini e delle unità monetarie vi sono ricamate.

Nei libri contabili della corte dei Tudor si trovano spesso, accanto agli addendi scritti in cifre arabe o romane, dei puntini, che dovevano servire allo scrivano come aiuti mnemonici nel trascrivere i risultati dei calcoli eseguiti sull'abaco.

Nell'amministrazione finanziaria questo metodo sopravvisse in molti stati fin verso la metà del XVIII secolo, in Francia fino alla rivoluzione, a Basilea fino al 1798.

5. *Abbandono dell'abaco e sua sopravvivenza.*

L'abaco costituí una premessa didattica per l'introduzione dei segni numerici arabi, in quanto in esso era implicitamente contenuto il valore posizionale. Per l'abaco stesso, tuttavia, l'introduzione delle cifre significò la fine, anche se questa fu molto piú lenta di quanto ci si sarebbe potuti attendere, e non senza ragione.

5.1. Scomparsa dell'abaco in Occidente.

Di per sé il caso dell'Italia dovrebbe essere tipico: l'introduzione delle cifre arabe, che papa Silvestro alla fine del X secolo applicò all'abaco, e che – duecento anni piú tardi – il Fibonacci indicava già come piú pratiche nella tecnica commerciale, determinò senz'altro la scomparsa dell'abaco. Né gli svariati *Libri d'abaco* né i numerosi *abachetti* (brevi manualetti di matematica elementare) menzionano l'abaco; non si ha notizia di alcun gettone coniato in Italia. L'Italia deve questa rapida e conseguente trasformazione alla sua posizione d'avanguardia nella tecnica finanziaria e nella contabilità medievali; o forse – e questo resta da vedere – il rapporto causale è inverso. Comunque, un autore italiano del XV secolo dice esser l'abaco in uso «hodie apud barbaros».

Nel resto dell'Europa il processo fu piú complesso. Una delle ragioni di ciò potrebbe essere il fatto che in quei paesi comparve l'abaco a linee orizzontali, assai piú pratico e sul quale il calcolo veniva eseguito piú speditamente. I mercanti italiani, inoltre, erano stabilmente in contatto con commercianti arabi, e ciò rese consueto l'uso delle cifre arabe. D'altra parte, la scrittura stessa era meno diffusa nell'Europa settentrionale che non in Italia.

A ciò vanno aggiunti i noti svantaggi delle cifre arabe, facili da contraffare e mal applicabili ai sistemi monetari e di misura non decimali; inoltre, l'alto costo della carta. Particolare difficoltà presentava poi la comprensione dello zero, ch'era considerato un segno – secondo quanto afferma uno scrittore tedesco dell'epoca – «che procura fatica e cagiona confusione».

Ma nel XVI secolo la svolta era ormai prossima. Maestri e manuali di calcolo propagavano il nuovo sistema, l'analfabetismo era in regresso. L'abaco cominciò con lo scomparire dalla contabilità privata: in Inghilterra, prima ancora della rivoluzione; nella tesoreria – la Exchequer Table – il cerimoniale sopravvisse tuttavia fino al 1785, e fino al 1826 si mantenne l'uso, in quello stesso ufficio, dei bastoncini con le tacche. In Olanda e in Belgio le ultime monete per far di conto furono coniate verso la fine del XVII secolo. In Germania l'abaco fu abbandonato all'inizio del XVIII secolo: il padre di Goethe ne faceva ancora uso.

Un manuale di calcolo francese del 1753 caratterizza l'uso dell'abaco come segue: «Questo modo di calcolare è piú praticato dalle donne che non dagli uomini; tuttavia molte persone occupate nelle Finanze... se ne servono con molto successo». Nella contabilità statale l'abaco sopravvisse ancora, per cader vittima della rivoluzione poco dopo il 1789.

5.2. Sopravvivenza dell'abaco in Oriente.

Può sorprendere che in tre grandi stati dell'Oriente – la Cina, il Giappone e la Russia – l'abaco abbia mantenuto, fino ad oggi, la sua importanza, benché le cifre arabe vi fossero conosciute. Il buono cede il passo al migliore, ma l'abaco orientale ha uguagliato in rapidità e duttilità il calcolo scritto.

Nel medioevo, tra il X ed il XII secolo, comparve in Cina lo *swan pan*, una forma razionalizzata di abaco, costituito da palline ordinate su cannucce di bambú o su fili; ogni ordine numerico è rappresentato con sette palline, cinque per le unità e due per le cinquine, separate da un listello di legno. Le quantità date vengono rappresentate sospingendo le palline contro il detto listello e, quando si sia raggiunto il valore di dieci, le palline vengono risospinte indietro per essere sostituite da una pallina dell'ordine superiore, che viene a sua volta sospinta contro il listello. Ciò consente una tale speditezza nell'esecuzione di calcoli semplici (benché, in teoria, il metodo sia analogo a quello descritto al § 3), che non soltanto l'addizione e la moltiplicazione scritte, ma anche la calcolatrice meccanica si rivelano piú lente.

Cosí, anche il giapponese *soroban*, ridotto a sei sole palline, e il russo *sčoty*, con dieci palline, sono indispensabili nelle banche, alle casse degli empori e dei negozi e nella contabilità domestica. Risultati ottenuti col calcolo scritto vengono ancora spesso controllati con l'abaco. Nelle scuole se ne insegna a tutt'oggi l'uso.

Tuttavia i giorni dell'abaco sono contati: esso sarà presto soppiantato dal calcolatore elettronico tascabile. In primo luogo proprio in Giappone, dove la produzione su vasta scala ne consente già la vendita a prezzi accessibili a tutti; quindi, in un futuro non lontano, anche in Russia, e finalmente in Cina.

6. *Eredità dell'abaco.*

Conformemente alla sua straordinaria importanza nella storia della civiltà, l'abaco ha lasciato piú tracce di quante generalmente non si creda. Nei musei si conservano naturalmente abaci greci in marmo, piccoli calcolatori in rame con dischetti mobili d'epoca romana, tavoli per il calcolo medievali originari dell'Europa centrale e dell'Inghilterra, panni e talvolta anche berrette che recano cucite delle cordicelle determinanti le colonne dei vari ordini numerici. Nelle collezioni numismatiche si trovano migliaia di monete per far di conto risalenti ai secoli XIII-XVIII, spesso con conî di grande interesse politico e storico-culturale. Piú importante è tuttavia l'eredità vivente.

6.1. Residui nel linguaggio.

In molte lingue europee la parola che designa l'attività del calcolare è ricavata dall'abaco. Il latino classico aveva *calculos ponere* 'porre sassolini', il latino medievale *calculare*, donde diverse lingue moderne (per esempio l'italiano e il francese) hanno ricavato l'espressione corrispondente. Altre lingue, a loro volta, hanno creato autonomamente una qualche locuzione, quali l'italiano *abbacare* e l'inglese *to cast* 'gettare [monete per far di conto]', oppure l'hanno impiegata per espressioni specifiche, come l'ungherese *számot vetni* 'computare' (letteralmente 'gettar numeri').

Anche il vocabolo internazionale *banca*, a designare un istituto finanziario, deriva dal banco (abaco) degli usurai e dei cambiavalute, il quale veniva – tra l'altro – pubblicamente infranto in caso di operato fraudolento (*bancarotta*). Il concetto di *bureau*, che in molte lingue è inteso come ufficio o studiolo, in francese ha ancora il senso primitivo di mobile, sul quale si scriveva e si eseguivano calcoli; in origine la parola designava però una coperta di rozza lana (franc. *bure*): un panno per far di conto.

Infine è da osservare che anche la parola *gettone* (franc. *jeton*) – che deriva dal fatto che le monete venivano gettate (franc. *jeter*) sulle linee dell'abaco – ha la sua origine in questo sistema di calcolo.

6.2. Vestigia culturali.

Non soltanto i semplici gettoni da gioco, ma tutta una serie di giochi di società rammentano l'abaco. Cosí il gioco inglese *Shove ha' penny*, oppure il *Pochbrett*, originario dell'Europa centrale, o il gioco della cordicella (*Schnurspiel*), popolare nelle regioni che costituirono un tempo la monarchia austro-ungarica. In tutti questi giochi si trattava di buttare o sospingere innanzi delle monete tra due linee.

Ancor piú significativo è il fatto che la notazione musicale, quale fu concepita da Guido d'Arezzo nell'XI secolo, ebbe a modello la configurazione dell'abaco: le linee del rigo corrispondono alle linee designanti gli ordini numerici, e le note ai gettoni.

7. *Conseguenze nella storia del pensiero.*

Si è definito l'abaco uno strumento che permette all'uomo di compiere le quattro operazioni fondamentali in modo che va oltre le sue facoltà biologiche. La meccanizzazione del procedimento di calcolo consente di effettuarlo in modo relativamente irriflesso. Invece nel calcolo scritto eseguito con le cifre arabe il cervello deve nuovamente essere portato ad un grado superiore di concentrazione.

In questo caso, dunque, lo svolgimento effettivo contraddice le leggi elementari della storia delle idee e della tecnica, secondo le quali, invece, l'uomo cerca di proiettare sul mondo esterno i propri sforzi sia fisici sia mentali, concretandoli in uno strumento meccanico.

Non deve dunque far meraviglia se già nel XV secolo vennero in uso le tavole di moltiplicazione (ted. *Rechenknecht*, franc. *barème*), se nel XVI furono inventati i logaritmi, ed infine, nel XVII, apparvero non solo le tavole di Nepero, ma anche le prime macchine calcolatrici. Quanto saldamente l'abaco fosse allora radicato nella cultura europea, lo mostra il fatto che due dei fondatori della matematica moderna, Pascal e Newton, eseguivano ancora su di esso i loro calcoli; entrambi costruirono però anche delle macchine calcolatrici.

Pascal, che aiutava il padre nella sua attività d'intendente di finanza, si convinse, considerando gli errori che si commettevano adoperando l'abaco, che la

riproduzione meccanica del procedimento mentale avrebbe portato a risultati ineccepibili. La sua macchina per eseguire addizioni di numeri fino ad otto cifre (1642) è la prima del genere in grado di funzionare.

Lo stesso Leibniz eseguiva ancora sull'abaco calcoli semplici ma, come Pascal, inventò una macchina calcolatrice – dotata di un già moderno congegno automatico di ruote a gradini –, ch'egli stesso definí un «abaco vivente», giacché grazie ad essa tutti i numeri si calcolavano, addizionavano, sottraevano, moltiplicavano e dividevano da soli. Con queste invenzioni comincia però la storia dei calcolatori elettronici digitali. [W. E.].

Strumento essenziale di un'attività – il **calcolo** – che precede ed anche resta indipendente dalla stessa **scrittura** (e cfr. **numero**), l'abaco serví a lungo e nelle piú diverse società ad eseguire rapidamente operazioni aritmetiche. Soltanto ora si può considerare definitivamente soppiantato dal calcolatore elettronico tascabile (cfr. **analogico/digitale**). La meccanicità delle operazioni eseguibili, fondamento della diffusione del suo uso pratico, può essere considerata riassorbita nel concetto attuale di **algoritmo**, nel quale ha ampio spazio l'esigenza di operare in un modo codificato (cfr. **codice**) con la maggior precisione possibile.

Algoritmo

La parola 'algoritmo' pare abbia origine dal nome del matematico persiano al-Khuwārizmī il quale formulò delle regole per il calcolo con le cifre decimali. La parola ebbe all'origine il significato di «calcolo mediante decimali»; attualmente ha un significato molto piú ampio, riferendosi anche a procedimenti di calcolo di natura assai diversa. Sarà dunque utile circoscrivere il significato del termine mediante una definizione, la cui legittimità risulterà dal corso dell'articolo.

DEFINIZIONE. *Si dice algoritmo una procedura effettiva, comune per una classe di dati iniziali, la quale trasformi, in un numero finito di passi elementari, i dati particolari nel risultato richiesto.*

I dati iniziali possono essere entità astratte arbitrarie, come simboli, successioni di simboli, numeri, figure geometriche, ecc. Una procedura è detta effettiva se può essere eseguita in maniera puramente meccanica, senza l'uso di inventiva od intelligenza. La classe di dati che possono essere trattati da un dato algoritmo è il suo *dominio*. La trasformazione dei dati mediante un algoritmo si effettua per passi elementari; ogni passo trasforma i dati assegnati in nuovi dati. Si crea cosí, a partire dai dati iniziali, una successione di risultati intermedi; l'ultimo elemento in questa successione è il risultato dell'algoritmo.

La definizione data, di cui si sono esplicitati i termini, può essere spiegata concettualmente mediante un esempio famoso: l'algoritmo di Euclide.

Il suo dominio è l'insieme di tutte le coppie di interi positivi; per ogni coppia il risultato da ottenersi è il massimo comun divisore (MCD) di questi interi. L'algoritmo è rappresentato da una lista di tre istruzioni che devono essere eseguite nell'ordine dato, iniziando con la prima istruzione della lista.

1) Si denoti il primo numero della coppia con x, il secondo con y.
2) Si calcoli il resto della divisione di x per y e lo si denoti con r.
3) Se r è uguale a zero, allora ci si arresti, il risultato è y. Altrimenti, si denoti y con x, r con y, e si torni alla istruzione 2.

L'azione dell'algoritmo di Euclide per la coppia (3542, 4140) può essere visualizzata mettendo in lista tutti i risultati intermedi, assieme ai numeri delle istruzioni che creano questi risultati:

Dati iniziali: 3542, 4140

1) x: 3542 y: 4140
2) x: 3542 y: 4140 r: 3542
3) x: 4140 y: 3542 r: 3542
2) x: 4140 y: 3542 r: 598
3) x: 3542 y: 598 r: 598
2) x: 3542 y: 598 r: 552
3) x: 598 y: 552 r: 552

2) x: 598 y: 552 r: 46
3) x: 552 y: 46 r: 46
2) x: 552 y: 46 r: 0
3) Il risultato è 46.

Come sarà dimostrato piú oltre, questo algoritmo agisce correttamente per tutti i dati iniziali assegnati.

La rappresentazione di un algoritmo mediante una lista di istruzioni è tipica. Abitualmente le istruzioni sono eseguite nell'ordine dato, a meno che il contenuto di una istruzione non si scosti dalla regola. Il numero di passi necessari per ottenere il risultato può variare in dipendenza dai dati iniziali, ma per qualsiasi scelta di questi, rimane finito. Ogni passo contiene qualche operazione sui dati; nell'esempio precedente queste operazioni sono o semplici operazioni aritmetiche, o operazioni di denominazione, ridenominazione, e confronto dei dati. Tutte possono essere compiute sia da esseri umani sia da dispositivi elettronici o meccanici.

L'algoritmo di Euclide agisce sui numeri; altri algoritmi agiscono su liste

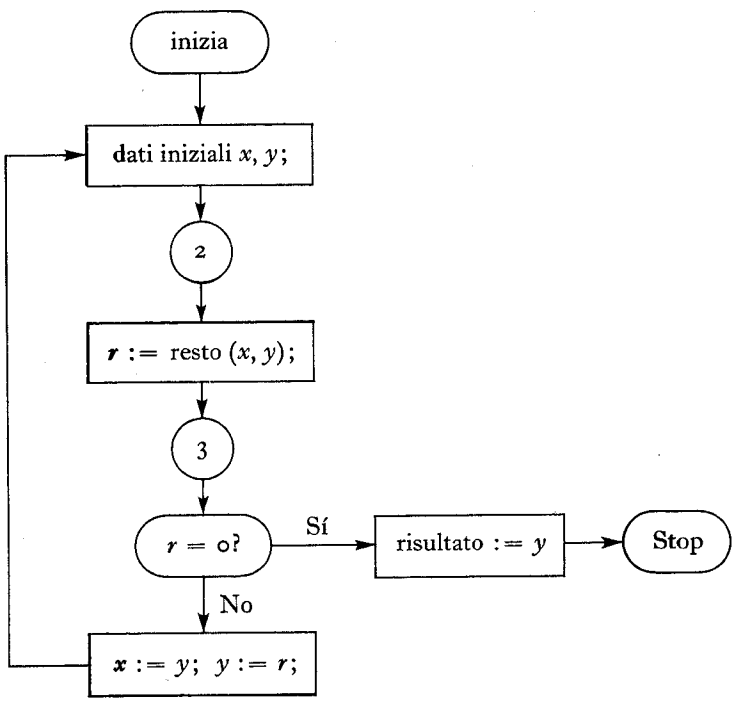


Figura 1.
Diagramma di flusso dell'algoritmo di Euclide.

di simboli, come gli algoritmi per le trasformazioni di espressioni, ad esempio per la semplificazione o la diversificazione; su grafi, come gli algoritmi per trovare il cammino piú breve in un grafo «pesato». Ben noti algoritmi per la moltiplicazione di matrici agiscono su tabelle di numeri; le costruzioni geometriche abituali non sono altro che algoritmi agenti su figure geometriche.

La caratteristica comune (e probabilmente la piú importante) di tutti gli algoritmi è la possibilità di eseguirli in modo meccanico. Una volta inventato, un algoritmo può essere usato da persone che non ne conoscono la sostanza, o perfino da un dispositivo, previa opportuna codificazione dei dati.

Gli algoritmi possono essere rappresentati in forma grafica (diagrammi di flusso) utile per capirli ed analizzarli (cfr. fig. 1).

Un tale metodo di rappresentazione, sebbene semplice e non richiedente spiegazioni, ha tuttavia due svantaggi: è difficile da formalizzare e può essere riconosciuto con difficoltà da dispositivi meccanici per il suo carattere bidimensionale. Sono stati inventati numerosi linguaggi formali per descrivere con precisione gli algoritmi. Un algoritmo, presentato in un tale linguaggio, è compreso sia da un essere umano sia da una macchina: si può fare l'esempio dell'Algol 60, un linguaggio formale elaborato nel 1958. Nell'Algol 60 gli algoritmi sono rappresentati mediante liste di simboli. Le costruzioni basilari di questo linguaggio sono affermazioni (esprimenti azioni) e dichiarazioni (descriventi i dati). La principale caratteristica dell'Algol 60 è la cosiddetta struttura a blocchi, che consente di trattare algoritmi in maniera gerarchica e logicamente elegante. L'algoritmo di Euclide scritto in Algol 60 ha la forma seguente:

```
begin integer x, y, r;
input (x); input (y);
if x≠0, y≠0 then
    begin a: r := remainder (x, y)
    if r = 0 then out (y) else
            begin x := y; y := r; go to a end
    end
end
```

I linguaggi formali creati per la descrizione di algoritmi sono detti *linguaggi algoritmici*. Un algoritmo scritto in tale linguaggio, congiuntamente con i dati assegnatigli, ha la forma di una lista di simboli e può essere trattato come un dato iniziale per un altro algoritmo che agisce nel modo seguente. Esso analizza la descrizione di un dato algoritmo, seguendo le regole della successione, compie azioni in accordo alle istruzioni incontrate, e si arresta quando trova l'istruzione **stop**. Non è difficile (in linea di principio) realizzare la costruzione di un algoritmo che possa dirsi *universale*. L'idea di un algoritmo universale ha profonde conseguenze pratiche; ne consegue che per l'esecuzione meccanica di algoritmi è sufficiente un solo dispositivo, cioè quello per la realizzazione dell'algoritmo universale. Ogni calcolatore universale digitale a programma è un esempio di un tale dispositivo. Poiché un calcolatore è un dispositivo concreto, e non astratto, è soggetto in pratica a limitazioni di spazio e tempo, e di conseguenza non tutti gli algoritmi possono essere effettivamente eseguiti con il suo aiuto. Tuttavia esso può eseguire una grande quantità di algoritmi «ragionevoli», purché scritti nel suo specifico linguaggio algoritmico.

Un algoritmo scritto in un tale linguaggio è un programma, e questo spiega perché si dice allo stesso modo «linguaggi algoritmici» e «linguaggi di programmazione». Non ogni programma tuttavia è la descrizione di un algoritmo; vi sono programmi che, per certi dati nel loro dominio, non si arrestano.

Trovare algoritmi, scriverli in linguaggio di programmazione, combinare parecchi algoritmi in un sistema, eseguirli mediante i calcolatori è la sostanza stessa della pratica che si riferisce ai calcolatori. Di conseguenza molte parti della scienza dei calcolatori, per esempio la progettazione architettonica mediante calcolatori, la teoria dei linguaggi di programmazione, la ingegneria *software* hanno alle spalle la nozione di algoritmo.

Dopo aver descritto un algoritmo, bisogna dimostrarne la correttezza, dimostrare cioè che, comunque scelti i dati nel suo dominio, l'algoritmo dà il risultato richiesto. Una tale dimostrazione consiste di solito di due parti; nella prima parte si prova che, se l'algoritmo si arresta, allora esso dà il risultato corretto (*correttezza parziale*); nella seconda parte si dimostra che l'azione dell'algoritmo si arresta per tutti i dati nel dominio (*arresto*). Dopo avere dimostrato queste due cose, si ha la dimostrazione della cosiddetta *correttezza totale*.

Il metodo piú noto per dimostrare la correttezza parziale di un algoritmo è quello delle asserzioni invarianti. Per spiegarlo, consideriamo ancora una volta l'algoritmo di Euclide. Supponiamo che i dati iniziali siano due interi positivi x_0, y_0. Bisogna dimostrare che il risultato (se esiste) è il massimo comun divisore di x_0, y_0 che indicheremo con $\text{MCD}(x_0, y_0)$. A tal fine, occorre dimostrare dapprima che i numeri indicati con x ed y soddisfano a $\text{MCD}(x, y) = \text{MCD}(x_0, y_0)$ *ogni volta* prima dell'esecuzione della istruzione 2. In effetti questa affermazione è vera dopo l'esecuzione della istruzione 1. Ora, assumendo che essa sia vera ad un certo stadio della esecuzione dell'algoritmo, in virtú delle leggi dell'aritmetica, ne segue che $\text{MCD}(x, y) = \text{MCD}(y, \text{resto}(x, y))$; allora, dopo avere ridenominato y con x, ed il resto della divisione di x per y con y, l'affermazione è ancora vera, e di conseguenza è invariante durante l'esecuzione dell'algoritmo. Nell'ultimo passo dell'azione, si ha $\text{resto}(x, y) = 0$, il che implica $y = \text{MCD}(x, y)$. Poiché in ogni momento $\text{MCD}(x, y) = \text{MCD}(x_0, y_0)$ allora $y = \text{MCD}(x_0, y_0)$, il che dimostra la parziale correttezza dell'algoritmo di Euclide.

Per dimostrare l'arresto, si usano argomentazioni di altro tipo. Si può osservare, in questo caso, che per ogni coppia di numeri positivi x_0, y_0 il numero denotato con r *decresce* ad ogni ritorno all'esecuzione della istruzione 3, rimanendo sempre non-negativo. Poiché non vi sono successioni decrescenti infinite di interi non-negativi, ne segue che la istruzione 3 è eseguita un numero finito di volte. L'algoritmo cioè deve arrestarsi, come volevasi dimostrare.

La dimostrazione precedente della correttezza totale dall'algoritmo di Euclide è facile e semplice. Tuttavia molti algoritmi d'interesse pratico sono piú complessi e la dimostrazione è un problema reale.

La dimostrazione della correttezza è solamente uno dei problemi nell'analisi matematica degli algoritmi. Un altro problema è l'analisi della complessità. Supponiamo che siano dati due diversi algoritmi, entrambi con lo stesso dominio, e che diano lo stesso risultato. Per decidere quale è il migliore, occorre una misura dell'efficienza dell'algoritmo, o, alternativamente, una misura della complessità dell'algoritmo.

Trovare una tale misura, che si accordi con la nostra intuizione, e poi paragonare gli algoritmi in accordo a questa misura è uno dei problemi piú importanti dell'analisi di complessità degli algoritmi. Quanto segue può dare un'idea di quali siano i problemi dell'analisi di complessità.

Una delle possibili misure di complessità è il numero dei passi eseguiti durante l'azione dell'algoritmo. Per confrontare due algoritmi rispetto a questa misura bisogna contare il numero dei passi per ogni scelta dei dati iniziali e per entrambi gli algoritmi, il che può non essere realistico. Invece, i dati possono essere classificati in accordo ad opportuni parametri e l'estremo superiore del numero dei passi, per ogni valore del parametro, può essere stimato per entrambi gli algoritmi. Se per ogni valore di questo parametro questo estremo superiore per il primo algoritmo è minore di quello del secondo, allora il primo algoritmo può essere considerato migliore. Come esempio di applicazione di questo criterio, consideriamo due algoritmi A e B con lo stesso dominio e che dànno lo stesso risultato: assegnata una lista non vuota di numeri crescenti ed un numero x, il risultato deve essere SÍ se x è nella lista e NO altrimenti.

Algoritmo A (ricerca sequenziale):

1) Si prenda il primo numero della lista e lo si confronti con x; se è uguale allora ci si arresti, il risultato è SÍ; altrimenti si scarti il primo numero dalla lista e si consideri la istruzione 2.
2) Se la lista è vuota, allora ci si arresti, il risultato è NO; altrimenti si torni alla istruzione 1.

Algoritmo B (ricerca binaria):

1) Se c'è solo un elemento nella lista, allora si consideri la istruzione 3; altrimenti si consideri la istruzione successiva.
2) Si indichi con m la parte intera del numero che denota la lunghezza della lista diviso per 2. Se x non è piú grande dell'elemento di posto m della lista, allora si scartino tutti gli elementi ad eccezione dei primi m della lista, altrimenti si scartino i primi m elementi della lista. Si ritorni alla istruzione 1.
3) Si paragoni x con il solo elemento della lista; se è uguale la risposta è SÍ, e ci si arresti; in caso contrario la risposta è NO e ci si arresti.

Prendiamo in esame per l'analisi solamente il numero di operazioni di confronto necessarie, invece del numero dei passi necessari. Sia n la lunghezza della lista, con $n \geq 1$. Allora il numero dei confronti fatto dall'algoritmo A, nel caso peggiore, è n, mentre questo numero per l'algoritmo B non supera mai $\log_2(n)+2$. Di conseguenza, per n sufficientemente grande è migliore l'algoritmo B. Anche considerando il numero totale dei passi, la stima precedente non cambierebbe sostanzialmente: per liste iniziali sufficientemente lunghe, l'algoritmo B richiede un minor numero di passi per completare la sua azione di quanti non siano necessari per A, entrambi considerati nel loro caso peggiore. In accordo con il criterio precedente l'algoritmo B è piú efficiente di A.

La nozione di algoritmo, intrinsecamente connessa con la nozione di effettività, non è stata analizzata solamente per ragioni pratiche. Sorgono in matematica questioni di natura filosofica riguardo a ciò che è possibile o non è possibile fare in modo effettivo.

Ad una prima considerazione pare infatti che ogni dimostrazione, ogni risultato della matematica sia riconducibile, almeno in linea teorica, ad un algoritmo. Soprattutto chi ha ricavato dalla matematica essenzialmente esperienze di tipo «calcolistico» può essere indotto a pensare in tale senso. Per mostrare come nella matematica trovino o possano trovare spazio anche argomentazioni di tipo diverso da quelle algoritmiche, si può menzionare un importante risultato, il teorema degli ideali primi.

Per esporre tecnicamente questo risultato sarebbe necessario soffermarsi preliminarmente sulle definizioni di anello, ideale, ideale primo, ideale massimale. Per non rendere la esposizione troppo gravosa, preferiamo fare qui libero uso di queste nozioni: quel che c'interessa, dando per scontata l'importanza del teorema, è una sua analisi critica.

Esso si può enunciare nel modo seguente:

TEOREMA. *Ogni anello $A \neq 0$ contiene almeno un ideale massimale.*

Si osserva come la dimostrazione di questo teorema contiene in maniera essenziale il seguente assioma (cui di fatto equivale):

ASSIOMA DI SCELTA. Assegnata una famiglia di insiemi $\{X_i\}$ è possibile scegliere simultaneamente uno ed un solo elemento x_i per ogni insieme X_i.

È evidente come questo assioma, facendo riferimento alla possibilità di dominare contemporaneamente delle scelte che possono essere anche infinite, è in completa opposizione con il concetto di algoritmo. D'altra parte vi sono molti e ragionevoli motivi per accettare questo assioma, non ultimo il teorema stesso, citato, che occupa nell'algebra un posto centrale.

Ne consegue dunque che un risultato fondamentale della matematica non è riducibile concettualmente ad un algoritmo. È chiaro come si apra qui un ampio spazio per discutere intorno alla natura della matematica. Se in essa privilegiamo la nozione di algoritmo, dovremo dare scarso peso al teorema citato e quindi rinunciare a una gran parte dell'algebra. Se viceversa riteniamo fondamentale questo teorema, dovremo accettare nella matematica accanto a procedimenti costruttivi anche affermazioni esistenziali, ossia procedimenti non-costruttivi. Il concetto di algoritmo viene di conseguenza ad avere un ruolo

importante ma non esaurisce l'intera matematica. Quale sia il giusto atteggiamento da tenere non è ovviamente una questione decidibile a priori, ma deve scaturire da un continuo confronto con l'esperienza. Ed è chiaro come differenti periodi storici possano condurre a situazioni e conseguentemente ad atteggiamenti diversi. A noi interessa qui avere posto, sia pure rudimentalmente, una problematica intorno al concetto di algoritmo ed alla sua eventuale identificazione con la matematica stessa.

Una questione di grande importanza circa il problema dei fondamenti della matematica è la seguente: esiste un algoritmo che possa decidere se una formula della teoria formale dei numeri è o meno valida? La risposta è negativa; un tale algoritmo non può esistere. Per dare una dimostrazione matematica di questa affermazione, occorre una definizione formale di algoritmo. Tale definizione è dovuta a Markov.

Sia A un insieme finito di simboli (*un alfabeto*) e si chiami *parola* ogni sequenza finita di simboli di A (si consentono anche le sequenze vuote). Le parole possono essere concatenate; la *concatenazione* della parola $(a_1, a_2, ..., a_n)$ con la parola $(b_1, b_2, ..., b_m)$ è la parola $(a_1, ..., a_n, b_1, ..., b_m)$. La parola $(a_1, ..., a_n)$ è scritta semplicemente $a_1a_2...a_n$. Se u e w sono parole, allora uw denota la concatenazione di u e w. La concatenazione è associativa. Se $w = w_1uw_2$ (con w_1 e w_2 eventualmente vuote), allora u è detta una *sottoparola* di w.

L'idea principale di Markov consiste nella seguente osservazione:

1) I dati sottoposti ad un procedimento effettivo possono essere rappresentati da parole di un alfabeto.
2) Ogni trasformazione effettiva di una parola può essere ridotta ad un numero finito di sostituzioni nella parola di alcune sue sottoparole mediante altre parole.

Questa osservazione conduce alla seguente definizione di algoritmo: algoritmo è una coppia (A, S), dove A è un alfabeto ed S una successione di istruzioni; ogni istruzione è della forma seguente:

$$u \to v \quad \text{(istruzione regolare)}$$

oppure

$$u \to \cdot v \quad \text{(istruzione terminale)}$$

dove u, v sono parole sopra A; i segni $\to$ e $\cdot$ non appartengono ad A. Si dice che l'istruzione $u \to v (u \to \cdot v)$ è applicabile alla parola w, se w contiene u come sottoparola. Data una parola che rappresenti dei dati, questa parola è trasformata mediante l'algoritmo a passo a passo in accordo con la regola seguente. Si trova la prima istruzione nella successione, applicabile alla parola; sia $u \to v$ (oppure $u \to \cdot v$); allora l'occorrenza piú a sinistra di u nella parola è sostituita con v, dando luogo ad una nuova parola intermedia. Se l'ultima istruzione applicata è terminale, oppure se non ci sono istruzioni applicabili alla parola nella successione, allora il procedimento ha termine; altrimenti si continua il procedimento.

Per esempio, l'algoritmo di Markov definito con l'alfabeto

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, (,), s$$

e la successione di istruzioni

$$\begin{array}{l} 0s \to \cdot 1 \\ 1s \to \cdot 2 \\ 2s \to \cdot 3 \\ 3s \to \cdot 4 \\ 4s \to \cdot 5 \\ 5s \to \cdot 6 \\ 6s \to \cdot 7 \\ 7s \to \cdot 8 \\ 8s \to \cdot 9 \\ 9s \to s0 \\ (s \to \cdot (1 \\ ) \to s) \end{array}$$

trasforma ogni intero non negativo scritto in forma decimale e chiuso tra parentesi nel suo successore scritto nella medesima forma.

La seguente successione di parole rappresenta l'azione di questo algoritmo per la parola iniziale '(5899)':

$$\begin{array}{ll} (5899) &) \to s) \\ (5899s) & 9s \to s0 \\ (589s0) & 9s \to s0 \\ (58s00) & 8s \to \cdot 9 \\ (5900) & \end{array}$$

A sinistra di ogni parola è data la prima istruzione applicabile alla parola assegnata.

Ci si potrà certo chiedere quale sia il senso di una procedura tanto complicata per un'operazione cosí facile quanto quella che consiste nel passare da un numero al successivo. La procedura ha un senso qualora si considerino i fondamenti dell'aritmetica: nella definizione dei numeri naturali data da Peano, infatti, la nozione di successore di un numero occupa un ruolo centrale.

Gli assiomi dei numeri naturali sono i seguenti:

- 0 è un numero naturale;
- se x è un numero naturale, esiste un altro numero naturale x', il successore di x;
- $0 \neq x'$ per ogni numero x;
- se $x' = y'$ allora $x = y$;
- data una certa proprietà Q che può valere o meno per tutti i numeri naturali, se essa vale per 0 e, ogni volta che vale per x vale per x', allora tutti i numeri naturali hanno la proprietà Q.

Da questi assiomi è agevole vedere come, con l'eccezione del primo, intervenga sempre la nozione di successore. Si capisce quindi come un'analisi in termini algoritmici della nozione di successore non sia frutto di un atteggiamento bizzarro, ma risponda ad un'esigenza reale; si ponga cioè nell'ottica di costruire in modo finitista l'aritmetica, almeno in parte. In altre parole si cerca di spingere ancora piú in profondità l'analisi di quali concetti siano necessari per ricavare il concetto di numero.

Markov afferma che ogni procedura effettiva di trasformazione di dati in risultati può essere rappresentata con un opportuno algoritmo della forma definita sopra. Questa affermazione non è un teorema, quindi non è possibile dimostrarla in termini matematici. Il motivo è la mancanza di precisione del termine 'effettivo'. Comunque, è stato dimostrato che altre definizioni di procedure effettive (ad esempio quelle dovute a Turing e Church) sono equivalenti a quella di Markov. Ciò depone a favore della validità dell'affermazione di Markov e indica che la definizione di Markov ben si adatta alla nostra idea intuitiva di effettività. Sulla base di questa definizione, la non-risolubilità di qualche problema può essere dimostrata.

Un problema (generale) si dice algoritmicamente non risolubile ovvero semplicemente, *non risolubile*, se non esiste un algoritmo che risolve ogni particolare istanza di questo problema. Il ben noto problema di corrispondenza di Post (PCP) è un esempio di problema non risolubile.

Due liste finite di parole su un alfabeto $(w_1, w_2, ..., w_n)$, $(u_1, u_2, ..., u_n)$, $n \geq 1$ si dicono avere la proprietà di Post, se esiste una successione di indici $i_1, i_2, ..., i_m$, $1 \leq i_j \leq n$, $1 \leq j \leq m$, $m \geq 1$, tale che $w_{i_1}w_{i_2}...w_{i_m} = u_{i_1}u_{i_2}...u_{i_m}$. Per esempio le liste (*b*, *bba*, *a*, *abb*), (*a*, *bab*, *ab*, *b*) hanno la proprietà di Post, poiché per la successione (3, 2, 1, 3, 4) le concatenazioni corrispondenti sono identiche, cioè entrambe sono la parola *abbabaabb*.

Ora il problema di corrispondenza di Post può essere formulato come segue. Sia dato un alfabeto composto di almeno due simboli. Per ogni coppia di liste finite di uguale lunghezza, aventi come elementi le parole sull'alfabeto dato, è da decidere se questa coppia abbia la proprietà di Post, oppure no.

È stato dimostrato che non esiste un algoritmo che per qualsiasi coppia di tali liste dia il risultato sí o NO in dipendenza dal fatto che essi abbiano la proprietà di Post oppure no. Di conseguenza, PCP non è risolubile. Molti risultati di non-risolubilità sono stati ottenuti attraverso la non-risolubilità del PCP. La dimostrazione standard di non-risolubilità di un dato problema è mostrare che la risolubilità di questo problema implicherebbe la risolubilità del PCP.

Esistono alcune generalizzazioni della nozione di algoritmo, importanti dal punto di vista teorico e/o pratico. Una tale generalizzazione è la nozione di algoritmo non-deterministico: un algoritmo è *non-deterministico* se durante la sua esecuzione la scelta di istruzioni successive è non-determinata; se cioè dopo l'esecuzione di un'istruzione, la successiva può essere scelta arbitrariamente in un insieme finito di possibili istruzioni.

Il seguente algoritmo (per cercare in un albero binario) è un esempio di algoritmo non-deterministico. I dati iniziali sono: un insieme finito di numeri, disposti in un albero binario, e un numero x. Il risultato è sí se x compare nell'albero.

1) Si prenda la radice dell'albero e la si denoti con v.
2) Se v è uguale a x, allora ci si fermi, ed il risultato è sí; altrimenti si prenda l'istruzione successiva.
3) Se v ha figli, allora si prenda l'istruzione 4 *oppure* l'istruzione 5; altrimenti ci si fermi, ed il risultato è POSSIBILE.
4) Si prenda il figlio piú vecchio di v, lo si denoti con v, e si ritorni all'istruzione 2.
5) Si prenda il figlio piú giovane di v, lo si denoti con v, e si ritorni all'istruzione 2.

L'istruzione responsabile del non-determinismo dell'algoritmo è l'istruzione 3. Usando questo algoritmo il risultato sí indica che x compare nell'albero; il risultato POSSIBILE non dà alcuna informazione.

La seconda generalizzazione è la nozione di algoritmo *concorrente*. In contrasto con l'usuale algoritmo (sequenziale), alcuni esempi di algoritmo concorrente possono essere eseguiti indipendentemente da tutti gli altri (concorrentemente); in tal modo, i risultati intermedi di un algoritmo concorrente non sono ordinati linearmente, come nel caso degli algoritmi sequenziali, ma sono ordinati solo parzialmente. Questa situazione riflette la possibilità di eseguire alcune trasformazioni definite con l'algoritmo, usando dispositivi che agiscono indipendentemente.

Il seguente algoritmo (per computare la somma di due interi positivi) è un esempio di algoritmo concorrente. I dati iniziali sono due interi positivi. Il risultato deve essere la loro somma.

1) Si denoti il primo numero con x ed il secondo con y.
2) Se y è uguale a 0 allora ci si fermi, il risultato è x; altrimenti si prenda l'istruzione 3 *e* l'istruzione 4.
3) Si calcoli $x+1$ e si denoti con x; si prenda l'istruzione 5.
4) Si calcoli $y-1$ e si denoti con y; si prenda l'istruzione 5.
5) Si attenda fin che le istruzioni 3 e 4 completino la loro azione; si prenda l'istruzione 2.

L'istruzione responsabile per la concorrenza di questo algoritmo è la 2, che inizia due azioni concorrenti; caratteristica per gli algoritmi concorrenti è anche l'istruzione 5 che sincronizza queste due azioni.

Concorrenza e non-determinismo sono nozioni completamente indipendenti e non debbono essere confuse; possono esservi algoritmi non-deterministici concorrenti, cosí come algoritmi deterministici concorrenti.

Va osservato che attualmente gli algoritmi non sono usati solamente per ottenere risultati finali. Talvolta è indagato un processo reale ed è possibile definire un algoritmo in modo tale che successivi risultati intermedi ottenuti durante la sua esecuzione rappresentino gli stadi successivi del processo reale. È possibile allora, osservando il comportamento dell'azione dell'algoritmo, mo-

strare alcune proprietà del processo. Questo uso degli algoritmi è noto come *simulazione* o *modellizzazione*. Gli algoritmi concorrenti sono particolarmente utili a tal fine. [A. M.].

Il termine, che indicava originariamente la pratica del **calcolo** resa possibile dall'introduzione delle cifre arabe (cfr. **numero e**, per altri modi di calcolo, **abaco**), è venuto ad assumere progressivamente un significato piú ampio, fino ad indicare qualsiasi procedimento effettivo che, all'interno delle **matematiche**, possa compiersi in un numero finito di passi (cfr. **ricorsività**). L'esempio della ricerca del massimo comun divisore (algoritmo di Euclide) permette di spiegare i vari termini scientifici e filosofici connessi al concetto di algoritmo (cfr. **automa, analogico/digitale, invariante, formalizzazione**). La definizione di algoritmo di Markov e il problema di Post stabiliscono naturalmente importanti legami non solo con le matematiche, ma anche con la **scienza** nel suo complesso (cfr. **applicazioni** e, per gli aspetti logico-filosofici, **determinato/indeterminato, logica**).

Approssimazione

1. Il concetto di approssimazione è intimamente legato al sorgere della scienza moderna ed acquista vigore e consistenza soprattutto a partire dal XVII secolo. Perché questo concetto possa svilupparsi, occorre infatti che la matematica s'imponga non solo nell'ambito delle concezioni scientifiche ma soprattutto in quello della vita pratica. Naturalmente anche prima di questa data la matematica occupava un posto importante, ma non comparabile rispetto a quanto avverrà poi. In effetti, se l'introduzione delle cifre arabe in Europa avviene all'inizio del XIII secolo (il *Liber Abaci* di Fibonacci è del 1202), l'aritmetica, il calcolo con le nuove cifre diverranno patrimonio comune solo gradualmente, e molto piú tardi.

Se per esempio si confronta la concezione che della scienza aveva Leonardo da Vinci – il quale pure poneva in grande rilievo il valore della matematica per descrivere la natura – con quella di Galileo si può osservare una grossa differenza qualitativa. Per Leonardo la matematica serve per esprimere, mediante rapporti, la natura delle cose; ma l'idea di effettuare misurazioni sistematiche, di valutare criticamente queste misure, in altre parole l'idea di «esperimento scientifico» è ancora in embrione. Con Galileo si avrà di essa chiara coscienza.

Un brano del famoso saggio di Alexandre Koyré intitolato programmaticamente *Du monde de l'« à-peu-près » à l'univers de la précision* [1961] illustra questa diversità: «In effetti, quando si studiano i libri di macchine dei secoli XVI o XVII, quando si fa l'analisi delle macchine (reali o semplicemente progettate) di cui essi ci offrono descrizioni e disegni, si è colpiti dal carattere approssimativo della loro struttura, del loro funzionamento, della loro concezione. Esse sono spesso descritte con le loro dimensioni (reali) esattamente misurate. In compenso non sono mai "calcolate". Anche la differenza tra quelle che sono irrealizzabili e quelle che sono state realizzate non consiste nel fatto che le prime siano state "mal calcolate", mentre le seconde lo sono state "bene". Né le une, né le altre lo sono state. Tutte – ad eccezione, forse, degli apparecchi di sollevamento e di qualche altro, come il mulino, che impiega per la trasmissione della forza motrice coppie di ruote di ingranaggio, mezzi che positivamente *invitano* al calcolo – sono state concepite ed eseguite "a occhio e croce", per stima. Esse appartengono, tutte, al mondo del "pressappoco"» (trad. it. p. 95).

Evidentemente c'è una grande differenza tra il contesto naturale che dà luogo a questa concezione della macchina e quello che si svilupperà successivamente all'interno della scienza moderna.

Il concetto di approssimazione, di valutazione critica degli errori non può essere presente in tutta la sua efficacia quando il calcolo ha solo una funzione secondaria all'interno della tecnologia. Cosí, nella scienza greca, nonostante il suo fiorire rigoglioso, il concetto di approssimazione non giunse a piena maturità. È sintomatico per esempio che, nonostante le grandi conquiste della matematica greca, non si dia all'interno di essa nulla di simile alla teoria degli errori. Questo può spiegarsi forse con il fatto che, nonostante l'originario

profondo contatto tra scienza e tecnologia, avvenga poi una separazione che privilegerà l'aspetto teorico.

È chiaro come in tale situazione non possa esservi spazio per una categoria concettuale cosí intimamente legata alla progressiva conquista del mondo reale come quella di approssimazione. In effetti lo sviluppo di una ricca ed efficace tecnologia è all'origine dello sviluppo della scuola di Mileto, come sottolinea Benjamin Farrington [1947] mostrando come le idee scientifiche di quei filosofi siano intrinsecamente legate ai primi ritrovati tecnologici: la ruota del vasaio, i mantici d'altoforno, il procedimento di filtratura. Sempre Farrington rileva come successivamente vi sarà una separazione della scienza stessa dalla tecnologia, dovuta essenzialmente alla schiavitú: «Dalla storia noi sappiamo che questi pregiudizi aumentarono tra i Greci con il sorgere della schiavitú. Piú essi credevano ai pregiudizi che questa generava e piú si tagliavano fuori dalle radici essenziali da cui viene succhiata la linfa della scienza. Staccata da tali radici la scienza greca diventò una pianta malata in cui l'elemento teorico rimase forte, ma quello pratico diminuito» (trad. it. p. 179).

Certamente con i filosofi della scuola di Alessandria è in atto una netta separazione tra scienza e tecnologia. Ctesibio, Filone ed Erone hanno lasciato descrizioni di macchine, di esperienze ingegnosissime dal punto di vista meccanico: oggetti rotanti, aperture automatiche di porte. È assente l'idea d'impiegare questi ritrovati tecnici al servizio della vita pratica; gli ingegnosi ritrovati dei filosofi, o meglio dei fisici citati, sono utilizzati come giocattoli, per allietare le feste con bizzarrie e curiosità.

L'esperienza descritta da Galileo nel brano che segue mostra un atteggiamento verso il mondo reale completamente diverso: anche se l'attrezzatura tecnica di cui dispone Galileo non è tutto sommato molto migliore di quella disponibile per un fisico greco del periodo alessandrino, vi è tuttavia di nuovo, e naturalmente in modo piú maturo, una tensione verso il mondo reale paragonabile a quella dei filosofi di Mileto.

«In un regolo o vogliàn dire corrente, di legno, lungo circa 12 braccia, e largo per un verso mezo braccio e per l'altro 3 dita, si era in questa minor larghezza incavato un canaletto, poco piú largo di un dito, tiratolo drittissimo e per averlo ben pulito e liscio, incollatavi dentro una carta pecora zannata, e lustrata al possibile, si faceva in esso scendere una palla di bronzo durissimo, ben rotondata e pulita; costituito che si era il detto regolo pendente, elevando sopra il piano orizzontale una delle sue estremità un braccio o due ad arbitrio, si lasciava (come dico) scendere per detto canale la palla, notando, nel modo che appresso dirò il tempo che consumava nello scorrerlo tutto, replicando il medesimo atto molte volte per assicurarsi bene della quantità del tempo, nel quale non si trovava mai differenza né anco della decima parte di una battuta di polso. Fatta e stabilita precisamente tale operazione, facemmo scendere la medesima palla solamente per la quarta parte di esso canale; e misurato il tempo della sua scesa, si trovava sempre puntualissimamente esser la metà dell'altro: e facendo poi l'esperienza di altre parti, esaminando ora il tempo di tutta la lunghezza col tempo della metà, o con quello delli due terzi o dei 3/4, o in conclusione con qualunque altra divisione per esperienze ben cento volte replicate sempre si incontrava, gli spazi passati esser tra di loro come i quadrati e i tempi, e questi in tutte le inclinazioni del piano, cioè del canale nel quale si faceva scendere la palla; dove osservammo ancora, i tempi delle scese per diverse inclinazioni mantenere esquisitamente tra di loro quella proporzione che piú abasso troveremo essergli assegnata e dimostrata dall'Autore. Quanto poi alla misura del tempo, si teneva una gran secchia piena d'acqua, attaccata in alto, la quale per un sottil cannellino saldatogli nel fondo, versava un sottil filo d'acqua che s'andava ricevendo con un piccol bicchiero per tutto 'l tempo che la palla scendeva nel canale e nelle sue parti: le particelle poi dell'acqua in tal guisa raccolte s'andavano di volta in volta con esattissima bilancia pesando, dandoci le differenze e proporzioni de i pesi loro le differenze e proporzioni de i tempi; e questo con tal giustezza che come ho detto, tali operazioni, molte e molte volte replicate, già mai non differivano d'un notabil momento» [Galilei 1638, ed. 1958 p. 199].

Si noti come l'intera descrizione sia permeata da un'esigenza di precisione. Le esperienze sono ripetute numerose volte, le misurazioni il piú possibile accurate. Il concetto di approssimazione è sicuramente presente, ed è chiaro come, con lo svilupparsi della scienza moderna e con la progressiva valutazione delle descrizioni *quantitative* dei fenomeni, acquisterà sempre maggior importanza. Si può dire infatti che caratteristica essenziale dello svilupparsi della scienza moderna sia, oltre alla rinunzia a spiegare le «cause» dei fenomeni, una ricerca di descrizione quantitativa di essi. Porre l'accento sulla misura e sulla misurabilità comporta necessariamente una valutazione critica della misura stessa, e quindi il sorgere di un concetto: quello di approssimazione.

Ma l'avere elevato a dignità concettuale l'approssimazione – con la conseguente valutazione dell'errore come qualcosa di intrinseco alla misura – ha conseguenze anche sulla concezione stessa della scienza. Con il XVII secolo, con la grande rivoluzione scientifica e filosofica, si giunge ad una concezione della scienza radicalmente diversa rispetto al passato: nasce l'idea di progresso scientifico. Scrive Paolo Rossi [1976, p. 69]: «Questa concezione della scienza [della scienza moderna] – che trova per la prima volta espressione, su un piano "filosofico", nell'opera di Francesco Bacone – giuoca un ruolo decisivo e determinante nella formazione dell'idea di progresso giacché essa implica: *a*) la convinzione che il sapere scientifico sia qualcosa che aumenta e che cresce, che si attua cioè attraverso un processo al quale contribuiscono, una dopo l'altra, le generazioni degli studiosi; *b*) la convinzione che questo progresso non sia mai, in uno qualunque dei suoi momenti o tappe, "completo": cioè non piú bisognoso di successive aggiunte o revisioni o integrazioni; *c*) infine la convinzione che si dia in qualche modo un'*unica* tradizione scientifica, che la scienza cioè non si presenti come un insieme di teorie contrapposte e di *ismi*, ma come un processo nel quale anche le svolte piú rivoluzionarie "salvano" il nucleo essenziale acquisito dalle generazioni precedenti, presentandosi come teorie piú generali che includono le teorie "vecchie" come loro casi particolari».

Paragonare il progresso scientifico ad una misura sempre piú accurata,

ad una esperienza compiuta con sempre maggior precisione, in altre parole ad una serie di «approssimazioni successive» non è un modo di procedere fortuito. Alla radice c'è lo stesso nucleo di pensiero, che concepisce l'errore come qualche cosa di inevitabile e di dominabile al tempo stesso. Questa concezione si rifletterà poi nella migliore tradizione filosofica occidentale, da Hegel alla teoria del rispecchiamento di Lenin.

Se si esamina, in particolare, il riflettersi della nuova concezione della scienza all'interno della matematica, è dato osservare che anche la nascita del calcolo differenziale può concepirsi come il risultato di «matematizzare» il concetto di approssimazione, in un caso specifico.

La geometria di Cartesio aveva fornito gli strumenti per introdurre il concetto di moto nel campo geometrico: naturalmente, non appena si considera un oggetto in movimento diviene di grande importanza anche considerare la «rapidità» del movimento stesso. Per descrivere matematicamente la «rapidità di movimento», in termine moderno la velocità, si può prendere come esempio la legge di caduta dei gravi di Galileo.

Tale legge si formula matematicamente con $s=4{,}9t^2$ ove s indica lo spazio percorso e t il tempo impiegato.

Se consideriamo, a partire da un certo tempo t_0 (nel quale vogliamo calcolare la «rapidità di movimento») un breve intervallo di tempo h, cioè immaginiamo che il tempo scorra da t_0 a t_0+h, lo spazio percorso sarà di conseguenza

$$s(t_0+h)-s(t_0)=4{,}9(t_0+h)^2-4{,}9t_0^2$$

Sarà cioè:

$$\begin{aligned} s(t_0+h)-s(t_0) &= 4{,}9(t_0^2+2t_0h+h^2)-4{,}9t_0^2= \\ &= \cancel{4{,}9t_0^2}+2\cdot 4{,}9t_0h+4{,}9h^2-\cancel{4{,}9t_0^2}= \\ &= 9{,}8t_0h+4{,}9h^2. \end{aligned}$$

La velocità media, che il mobile tiene nell'intervallo (t_0, t_0+h) (spazio/tempo) sarà perciò:

$$\frac{s(t_0+h)-s(t_0)}{h}=\frac{9{,}8t_0h+4{,}9h^2}{h}=\frac{(9{,}8t_0+4{,}9h)\,h}{h}=$$
$$=9{,}8t_0+4{,}9h.$$

Se ora si pensa ad intervalli di tempo sempre piú piccoli, cioè a valori di h che si avvicinano sempre piú a 0, si avrà che il valore della velocità media si avvicina sempre piú al valore di $9{,}8t_0$. Questo valore dà nell'istante t_0 la «rapidità di mutamento», in termini moderni la velocità.

La velocità all'istante t_0 è dunque definita come il valore al quale «si approssimano sempre piú» le velocità medie.

Ciò che si è ottenuto – la derivata della funzione $s=4{,}9t_0^2$ al tempo t_0 – può essere esteso a qualsiasi altra situazione ove compaia una relazione funzionale; è possibile cioè calcolare la rapidità istantanea di variazione di una variabile y rispetto alla variabile x e si ha cosí il concetto matematico di derivata.

L'ipotesi che vi sia una stretta connessione tra il concetto di approssimazione ed il concetto matematico di derivata è espressa, per esempio, da Carnot [1797]: «La difficoltà che si incontra spesso a esprimere esattamente i diversi dati d'un problema con delle equazioni, e a risolvere queste ancora, ha potuto far nascere le prime idee del calcolo infinitesimale. Infatti allorché è troppo difficile trovar la soluzione esatta d'una quistione, egli è naturale di tentare almeno d'approssimarsene piú che sia possibile trascurando le quantità, che imbarazzano le combinazioni, purché si prevegga che queste quantità trascurate non possono, atteso il loro picciol valore, produrre che un error parimenti trascurabile nel risultato del calcolo» (trad. it. p. 3).

Si badi tuttavia che il legame tra approssimazione e calcolo differenziale è solamente ideale, e non va inteso nel senso riduttivo che la derivata sia, in qualche modo, una grandezza approssimata.

In opposizione all'idea che la derivata sia un misurare empirico, ove si trascurano certi elementi ritenuti troppo piccoli, vale la pena di citare il seguente passo di Hegel [1812]: «Se la condiscendenza dell'ordinario intelletto permette una simile imprecisione, tutti i geometri all'incontro hanno rigettato questa rappresentazione. Salta agli occhi di per sé che nella scienza della matematica non si parla, né tanto né poco, di cotesta precisione empirica, e che il misurare matematico per mezzo delle operazioni del calcolo oppure delle costruzioni della geometria, differisce intieramente dall'agrimensura e dalla misurazione di linee e figure empiriche etc.» (trad. it. p. 286).

Si vedranno in seguito altri aspetti matematici dell'approssimazione; per il momento importa aggiungere qualche considerazione sul suo significato scientifico generale.

Se si è insistito in precedenza sul fatto che il concetto di approssimazione *non* è un semplice risultato dello sviluppo tecnologico, non è stato certo per proporre una concezione della scienza avulsa dal mondo reale, ma piuttosto per sottolineare il fatto che i rapporti con esso sono molto piú intricati e problematici che non una semplice dipendenza a senso unico del tipo struttura-sovrastruttura.

Cosí la realizzazione di un orologio efficiente – esigenza indispensabile per la navigazione in alto mare, poiché per determinare la longitudine occorre avere con sé l'ora del meridiano d'origine – non è legata alla pratica degli orologiai, ma agli sviluppi di una teoria scientifica: ovviamente questa teoria trae origine da esigenze della vita pratica, ma quello che preme sottolineare è che il ritrovato tecnologico in questione non è immediatamente dedotto dall'istanza pratica. Scrive Koyré [1961]: «Non è tuttavia dall'orologio degli orologiai che è venuto finalmente fuori l'orologio di precisione. L'orologio degli orologiai non ha mai superato – né lo poteva – lo stadio del "quasi" e il livello del "pressappoco". L'orologio di precisione, l'orologio cronometrico ha tutt'altra origine. Esso non è in nessun modo una promozione dell'orologio d'uso pratico. Esso è uno *strumento*, cioè una creazione del pensiero *scientifico*, o, meglio ancora, la realizzazione cosciente di una teoria» (trad. it. p. 106). E poco oltre: «Ma non è l'utilizzazione di un oggetto che ne determina la natura: è la struttura. Un cro-

nometro resta un *cronometro* anche se lo adoperano dei marinai. E questo ci spiega perché le grandi invenzioni decisive risalgano non agli orologiai, ma ai sapienti; non a Jost Burgi e a Isaak Thuret, ma a Galileo e a Huygens (e anche a Robert Hooke), ai quali dobbiamo l'orologio a pendolo e l'orologio a spirale» [*ibid.*, p. 107].

Con la nascita della nuova scienza, alla quale è intimamente legato il concetto di approssimazione, si pone dunque il problema di strumenti di misura sempre piú efficaci. Per la concezione classica spiegare un fenomeno fisico significava, dopo avere effettuato certe ipotesi semplificatrici, trovarne la sua causa. Per la scienza moderna, che ha rinunziato alle «cause», si tratta invece di fornire di esso una descrizione *quantitativa* precisa quanto piú possibile. È questa la «legge» del fenomeno e ad essa deve esaurirsi la spiegazione.

L'esigenza di misure sempre piú precise diventa in tal modo una componente importante del pensiero scientifico e tecnologico. Basti pensare all'estrema importanza della precisione, dell'attendibilità dei dati nell'attuale tecnologia. Ma anche nel pensiero scientifico attuale misurazioni precise, esperimenti di grande accuratezza hanno la piú grande importanza. E persino, sul piano filosofico, la tesi di Popper che sia auspicabile per una teoria un alto grado di falsificabilità, o di controllabilità, sembra, in ultima analisi, un riflesso della preoccupazione di organizzare esperimenti che siano controllabili con la maggior accuratezza possibile.

Conseguenza di tutto ciò è anche la necessità di una teoria dell'approssimazione. Se si considera infatti una celebre esperienza fisica, quella di Michelson, che ebbe un contributo decisivo nel demolire il concetto di etere, essa passa attraverso la mediazione di uno strumento sensibilissimo, l'interferometro, e richiede tra i suoi dati la velocità della luce nel vuoto e la velocità di rivoluzione della Terra intorno al Sole. Queste due velocità devono quindi essere calcolate con la massima accuratezza e si richiedono strumenti teorici che consentano di affrontare e dominare calcoli numerici di grande complessità. In altre parole non è possibile pensare ad una scienza e ad una tecnologia avanzate senza una buona teoria dell'approssimazione. In questo articolo si tratterà di alcuni aspetti matematici della teoria dell'approssimazione, per poi svilupparne un particolare aspetto nell'ambito della matematica attuale.

Si è già visto come il concetto di approssimazione sia intimamente legato ai fondamenti stessi del calcolo differenziale, ossia al concetto di derivata. Anche una formula fondamentale di questo calcolo, la formula di Taylor, è legata a questo concetto, e sarà il caso di illustrarla brevemente.

Se si considerano diverse espressioni analitiche (diverse funzioni) quali

$$x+1 \qquad x^2+3x \qquad \frac{\sqrt{x}+x}{\operatorname{sen} x} \qquad \log(1+x^2)$$

si è subito colpiti dal fatto seguente: per calcolarne il valore in qualche punto, ad esempio per $x=1$, dobbiamo affrontare diverse difficoltà a seconda della funzione.

Si ha facilmente per le prime due:

$$1+1=2 \qquad 1^2+3\cdot 1=4$$

ma per le altre due abbiamo

$$\frac{\sqrt{1}+1}{\operatorname{sen}(1)}=\frac{2}{\operatorname{sen} 1} \qquad \log(1+1^2)=\log 2$$

e non possiamo esplicitare maggiormente il valore numerico senza qualche ulteriore aiuto, ad esempio delle tavole di logaritmi.

Cosa rende particolarmente facile trattare le prime due funzioni (per $x=1$ o per qualsiasi altro valore)? La loro forma: esse sono polinomi, cioè espressioni che appartengono al tipo generale

$$a_0+a_1x+a_2x^2+\ldots+a_nx^n.$$

L'idea della formula di Taylor è ora che, «nell'intorno di un punto x_0», cioè per valori della variabile x abbastanza vicini a x_0, una funzione $f(x)$ possa essere ben approssimata da un polinomio di grado n, tenendo conto del valore della funzione nel punto x_0, $f(x_0)$ e delle sue n derivate $f'(x_0)$, $f''(x_0)$, ..., $f^{(n)}(x_0)$.

Questa idea conduce alla formula:

$$(*) \qquad f(x)=f(x_0)+\frac{x-x_0}{1!}f'(x_0)+\frac{(x-x_0)^2}{2!}f''(x_0)+\ldots+\frac{(x-x_0)^n}{n!}f^{(n)}(x_0)+\varepsilon$$

ove naturalmente il «resto» ε è della massima importanza.

Se, supponendo x non troppo discosto da x_0, si riesce a fare in modo che questo resto sia abbastanza piccolo, in modo da essere trascurato nei calcoli, la espressione (*) ci permette di considerare $f(x)$ come un polinomio.

Se supponiamo, ad esempio, che esista anche la derivata $(n+1)$-esima di $f(x)$ nell'intervallo (x_0, x) allora ε non può superare il valore massimo della funzione

$$|f^{(n)}(\alpha)(x-x_0)^n/n!|$$

per α variabile in (x_0, x). In altre parole se noi conosciamo dei limiti per $f^{(n)}(x)$ possiamo circoscrivere l'errore.

È chiara l'importanza di una formula di questo genere, ad esempio per il calcolo numerico.

L'idea che si è vista esplicitarsi per giungere alla formula di Taylor, di sostituire ad una funzione un polinomio ricavandone le caratteristiche dal comportamento «locale» della funzione, può applicarsi ad altre situazioni.

Si veda il risultato noto come «teorema fondamentale della teoria della interpolazione».

Sia $f(x)$ una funzione definita nell'intervallo $[a, b]$.

Possiamo proporci di approssimare $f(x)$ mediante un polinomio di grado n imponendo però questa volta che il polinomio assuma in certi punti x_0, x_1, ..., x_n esattamente i valori della funzione $f(x)$, cioè $f(x_0)$, $f(x_1)$, ..., $f(x_n)$.

Siamo cosí condotti al problema di determinare un polinomio

$$p(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$$

tale che

$$\begin{array}{c} a_0+a_1x_0+\ldots+a_nx_0^n=f(x_0) \\ \vdots \qquad \vdots \qquad\qquad \vdots \qquad \vdots \\ a_0+a_1x_n+\ldots+a_nx_n^n=f(x_n) \end{array}$$

L'esistenza di questo polinomio segue immediatamente osservando come il determinante

$$\begin{vmatrix} 1 & x_0 & \ldots & x_0^n \\ 1 & x_1 & \ldots & x_1^n \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \ldots & x_n^n \end{vmatrix}$$

debba essere diverso da zero. Questo è il teorema fondamentale citato sopra. Si noterà come si sia data una pura dimostrazione di esistenza del polinomio $p(x)$; il problema della sua costruzione effettiva va affrontato con tutt'altre tecniche sulle quali non ci si soffermerà in questa sede.

Se supponiamo che $f(x)$ sia derivabile fino all'ordine $(n+1)$ nell'intervallo $[a, b]$, è possibile dimostrare come sia

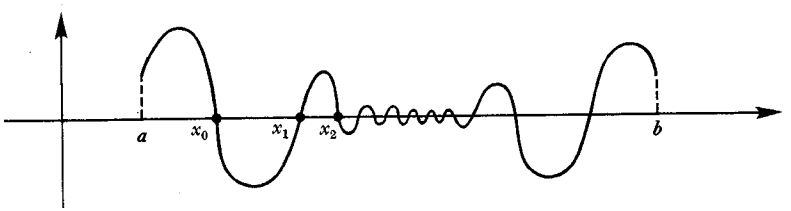
$$\left|f(x)-p(x)\right| \leq \frac{M^{n+1}}{(n+1)!}\left|(x-x_0)(x-x_1)\ldots(x-x_n)\right|$$

ove M^{n+1} è una limitazione superiore per $f^{(n+1)}(x)$ in (a, b).

Notiamo ancora come la formula di Taylor e la interpolazione mediante un polinomio di grado n per $n+1$ punti del grafico della funzione siano, in realtà, espressioni della stessa idea. La formula di Taylor si riferisce al caso limite nel quale gli $n+1$ punti vengono fatti coincidere in x_0, il che comporta esattamente avere assegnate derivate in x_0, fino all'ordine n.

Procedendo in questo ordine d'idee si pone immediatamente il problema di minimizzare l'errore aumentando il numero dei valori $x_0, x_1, \ldots, x_n$, presi in esame. È lecito attendersi approssimazioni sempre migliori al crescere dei valori considerati.

Tuttavia cosí il problema è posto con molta ingenuità; se infatti consideriamo una funzione $f(x)$ che abbia infiniti zeri in (a, b)



e scegliamo i valori $f(x_0)=f(x_1)=\ldots=f(x_n)=\ldots=0$, otteniamo il polinomio nullo che non è affatto una buona approssimazione! Si capisce cosí come sia necessario imporre ulteriori condizioni e/o scegliere oculatamente i valori (nodi) nei quali si impone la coincidenza della funzione data con il polinomio approssimante.

Senza soffermarsi ulteriormente sui vari particolari aspetti connessi ad approssimazioni specifiche in casi speciali, si esporranno ora per sommi capi alcune questioni di quella che, all'interno della matematica, viene denominata teoria dell'approssimazione. [M. G.].

2. In numerosi problemi gli oggetti investigati e le loro descrizioni approssimative possono essere identificati con gli elementi di uno spazio metrico X, e l'errore commesso prendendo la osservazione approssimativa $\tilde{x}$ dell'oggetto osservato x può essere identificato con la distanza $\rho(\tilde{x}, x)$ tra gli elementi $\tilde{x}$ ed x. Sia $Z \subset X$ un dato sottoinsieme dello spazio metrico X; questo insieme può essere identificato con la classe degli oggetti investigati. Si denoti con X_h il sottoinsieme delle descrizioni approssimate degli elementi di Z, ottenute usando dei metodi di osservazione indiciati da h. Denotiamo con H l'insieme di tutti gli indici dei metodi usati per le indagini. Supponiamo che per ogni $\varepsilon>0$ si voglia determinare la classe dei metodi che approssimano gli elementi di Z con errore non piú grande di ε. Questo problema, di ovvia importanza pratica, può essere formulato nel modo seguente:

PROBLEMA 1. Trovare un sottoinsieme $H_\varepsilon \subseteq H$ tale che per ogni $x \in Z$ e per ogni $h \in H_\varepsilon$ esista un $x_h \in X_h$ tale che $\rho(x, x_h) \leq \varepsilon$.

Una soluzione del problema 1, se esiste, dipende dal numero ε, il quale, in ogni problema, è determinato dalla precisione richiesta per il nostro studio. Prescindendo da tale formulazione particolare del problema, consideriamo il seguente problema piú generale:

PROBLEMA 2. Sia H un sottoinsieme di $(0, 1]$ tale che $\inf H=0$ e sia $\{X_h\}_{h\in H}$ una famiglia di sottoinsiemi di X. Per ogni $x \in Z$ trovare una famiglia $\{x_h\}_{h\in H}$ tale che per ogni $h \in H$ e $x_h \in X_h$ si abbia $\lim_{h\to 0} \rho(x, x_h)=0$.

Se esiste una soluzione del problema 2, cioè la famiglia $\{x_h\}_{h\in H}$, allora l'insieme $H_\varepsilon = H \cap (0, h_\varepsilon)$ è una soluzione del problema 1, ove h_ε è definito da $h_\varepsilon = \inf_{x\in Z}[h \mid \rho(x, x_h) \geq \varepsilon]$.

Il problema 2 è il problema fondamentale della teoria dell'approssimazione.

1. *Approssimazione di insiemi in uno spazio metrico.*

Se il problema 2 è risolubile, la famiglia $\{X_h\}_{h\in H}$ è detta l'approssimante dell'insieme $Z \subset X$, quindi $\{X_h\}_{h\in H}$ è l'approssimante se per ogni $z \in Z$ e per ogni $h \in H$ esiste $x_h \in X_h$, che perciò indicheremo con $x_h(z)$, tale che $\lim_{h\to 0} \rho(z, x_h(z))=0$.

Generalmente, non ogni famiglia di sottoinsiemi nello spazio metrico X forma l'approssimante dell'insieme dato $Z \subset X$, cioè non ogni famiglia $\{X_h\}_{h \in H}$ ammette una soluzione al problema 2.

Una volta dato l'approssimante dell'insieme Z, la costruzione di una soluzione del problema 2 si fonda sopra la determinazione della famiglia $\{p_h\}_{h \in H}$ di funzioni, $p_h : Z \to X_h$ che soddisfano la condizione: $\lim_{h \to 0} \rho(z, p_h(z)) = 0$, per ogni $z \in Z$.

Se $\{X_h\}_{h \in H}$ è l'approssimante di Z e la famiglia $\{p_h\}_{h \in H}$ soddisfa la condizione stabilita sopra, la famiglia di coppie $\{X_h, p_h\}_{h \in H}$ è detta l'approssimazione dell'insieme $Z \subset X$.

L'errore dell'approssimazione dell'elemento $z \in Z$ è determinato con il funzionale e_h, $e_h(z) = \rho(z, p_h(z))$, per ogni $h \in H$.

Per il dato approssimante $\{X_h\}_{h \in H}$ possiamo in generale trovare molte differenti approssimazioni $\{X_h, p_h\}_{h \in H}$ dell'insieme Z. Ma nel caso in cui gl'insiemi X_h siano chiusi per tutti gli $h \in H$, l'approssimazione ottimale $\{X_h, \mathring{p}_h\}_{h \in H}$ può essere distinta con le relazioni: per ogni $z \in Z$ e per ogni $h \in H$ e per ogni $x_h \in X_h$: $\rho(z, \mathring{p}_h(z)) \leq \rho(z, x_h)$.

Il piú noto esempio di approssimazione è dato dallo sviluppo decimale finito dei numeri reali. Si prenda come X l'insieme di tutti i numeri reali con la distanza definita da $\rho(x, y) = |x - y|$, e sia Z l'intervallo $[0, 1)$. Se noi poniamo:

$$H = [h | h(n+1) = 1, \ n = 0, 1, \ldots]$$
$$X_h = [y | y = k\, 10^{-n}, \ k = 0, 1, \ldots, 10^n, \ h(n+1) = 1]$$

allora possiamo verificare che $\{X_h\}_{h \in H}$ è l'approssimante di Z.

Se $\{p_h\}_{h \in H}$ è definito dalle relazioni $p_h(x) = 10^{-n}$ parte intera $(x\, 10^n)$, per $h(n+1) = 1$ ed ogni $x \in Z$, allora per ogni $x \in [0, 1)$ si ha $e_h(x) = |x - p_h(x)| = x - p_h(x) < x - 10^{-n}(x\, 10^n - 1) = 10^{-n}$, il che dimostra che $\lim_{h \to 0} e_h(x) = 0$ e che la famiglia $\{X_h, p_h\}_{h \in H}$ è l'approssimazione di $Z = [0, 1)$.

È facile provare che, ponendo $\mathring{p}_h(x) = 10^{-n}$ parte intera $(x\, 10^{-n} + \frac{1}{2})$, per $h(n+1) = 1$ e ogni $x \in [0, 1)$ otteniamo l'approssimazione ottimale $\{X_h \mathring{p}_h\}_{h \in H}$ dell'insieme $Z = [0, 1)$.

Un altro esempio assai importante è l'approssimazione polinomiale dell'insieme $C[0, 1]$ di tutte le funzioni reali continue sull'intervallo chiuso $[0, 1]$. Assumiamo come spazio metrico X l'insieme $C[0, 1]$ con la distanza definita da $\rho(x, y) = \sup_{t \in [0,1]} |x(t) - y(t)|$.

Sia H ancora l'insieme, $H = [h | h(n+1) = 1, \ n = 0, 1, \ldots]$ e $X_h = \mathrm{Lin}\{1, t, t^2, \ldots, t^n\}$* per $h(n+1) = 1$, $n = 0, 1, \ldots$, ossia l'insieme dei polinomi di grado n.

Ponendo: $p_h x(t) = \sum_{m=0}^{n} \binom{n}{m} x \binom{m}{n} t^m (1-t)^{n-m}$ per $h(n+1) = 1$ e per ogni $x \in C[0, 1]$, si definisce il polinomio di Bernstein di grado n e $\lim_{h \to 0} \rho(x, p_h x) = 0$ per il teorema di approssimazione di Weierstrass [Yosida 1974]. Ne segue di

* Con $\mathrm{Lin}(Z)$ indichiamo il piú piccolo insieme lineare in X che contiene $Z (Z \subset X)$. L'insieme $\mathrm{Lin}(Z)$ è detto inviluppo lineare dell'insieme Z [cfr. Kantorovich e Akilov 1964].

conseguenza che la famiglia $\{X_h, p_h\}_{h \in H}$ è un'approssimazione dello spazio $C[0, 1]$.

Ricercando una approssimazione del sottoinsieme Z nello spazio metrico X, dobbiamo risolvere i due problemi seguenti:

A) Dato in uno spazio metrico il sottoinsieme Z, trovare un approssimante $\{X_h\}_{h \in H}$ di Z.

B) Dati in uno spazio metrico X il sottoinsieme Z e il suo approssimante $\{X_h\}_{h \in H}$, trovare la famiglia di funzioni $\{p_h\}_{h \in H}$ tali per ogni $h \in H$, $p_h : Z \to X_h$ e per ogni $x \in Z$, $\lim_{h \to 0}(x, p_h x) = 0$.

La soluzione dei problemi A e B, negli spazi metrici generali, non è conosciuta. Risultati relativamente completi sono stati ottenuti negli spazi lineari normati [cfr. Singer 1970].

Qui noi discutiamo brevemente solamente l'approssimazione degli spazi di Banach, restringendo le nostre considerazioni al caso in cui gli approssimanti siano formati da sottospazi lineari di dimensione finita. Questo sembra il caso piú importante per le applicazioni pratiche.

2. *Approssimazione di uno spazio di Banach con sottospazi di dimensione finita.*

Se X è uno spazio di Banach separabile, allora esiste un insieme numerabile $\{x_j\}_{j=0}^{\infty}$ denso in X.

Poniamo $H = [h | h(n+1) = 1, \ n = 0, 1, \ldots]$ e $X_h = \mathrm{Lin}\{x_0, \ldots, x_n\}$* per $h(n+1) = 1$, $n = 0, 1, \ldots$; si vede che $\{X_h\}_{h \in H}$ è l'approssimante di X ed ogni X_h è un sottospazio di X di dimensione finita. Quindi ogni spazio di Banach separabile ha l'approssimante composto di sottospazi di dimensione finita.

L'approssimante che è stato costruito in questo modo, tuttavia, non è vantaggioso nella pratica, perché contiene sottosequenze composte del medesimo sottospazio di X. Di conseguenza spesso si costruisce un approssimante partendo dalle basi algebriche [cfr. Kantorovich e Akilov 1964] dello spazio X, se queste basi esistono e sono date ed hanno proprietà ulteriori utili per studiare certe classi di problemi [cfr. Aubin 1972].

Discutiamo ora il problema B, assumendo che l'approssimante $\{X_h\}_{h \in H}$ dello spazio di Banach X sia dato. Ricercheremo una famiglia di applicazioni $\{p_h\}_{h \in H}$ che soddisfi le seguenti due condizioni:

I) per ogni $h \in H$ e per ogni $x \in X_h$, $p_h x = x$.

II) per ogni $h \in H$ si ha $p_h : X \to X_h$ e p_h è lineare e limitata.

Questo significa che $p_h p_h = p_h$ cioè che per ogni $h \in H$, p_h è una proiezione lineare su un sottospazio di dimensione finita X_h. È facile dimostrare che tutte queste applicazioni sono della forma: $p_h x = \sum_{j=1}^{d_h} r_{hj}(x) x_{hj}$, per tutti gli $x \in X$, do-

* Cfr. la nota alla pagina precedente.

ve $d_h = \dim X_h$, $\{x_{hj}\}_{j=1,\dots,d_h}$ è la base di X_h, cioè $X_h = \mathrm{Lin}\{x_{h1}, \dots, x_{hd_h}\}$, e $r_{h1}, \dots, r_{hd_h}$ sono funzionali lineari continui su X, che soddisfano la condizione di biortogonalità:

$$r_{hj}(x_{hk}) = \delta_{jk}, \text{ per } j, k = 1, 2, \dots, d_h, \quad \delta_{jk} = \begin{cases} 1 & \text{se } j = k \\ 0 & \text{se } j \neq k. \end{cases}$$

Assumiamo che la famiglia $\{p_h\}_{h \in H}$ definita da I) e II) sia uniformemente limitata, cioè

(K) Esiste una costante K, $0 < K < \infty$ tale che per ogni $h \in H$, $\|p_h\| \leq K$.

Allora per ogni $v \in X_h$, $p_h v = v$, e per ogni $x \in X$,

$$p_h x - x = p_h x - p_h v + v - x = (p_h - I)(x - v);$$

cosí

$$\|p_h x - x\| \leq (1 + K)\|x - v\|.$$

Ne consegue finalmente che esiste una costante reale positiva C, tale che per ogni $h \in H$ e per ogni $x \in X$

$$\|p_h x - x\| \leq C \inf_{v \in X_h} \|x - v\|.$$

In altre parole, se le condizioni I), II) e (K) sono verificate la famiglia $\{X_h, p_h\}_{h \in H}$ è l'approssimazione di X, a patto che $\{X_h\}_{h \in H}$ sia l'approssimante di X. Inoltre l'errore di approssimazione è uniformemente maggiorato dall'errore dell'approssimazione ottimale.

Osservazione. Per il teorema di Banach-Steinhaus possiamo sostituire la condizione (K) mediante la seguente condizione (K'):

(K') Per ogni $x \in X$ esiste un numero reale positivo K tale che per ogni $h \in H$, $\|p_h x\| \leq K$.

Vale la pena di notare che non per tutti gli approssimanti possiamo trovare delle approssimazioni che soddisfano I), II) e (K). È stato trovato da Lozinsky e Haršiladze [Singer 1970] che l'approssimante $\{X_h\}_{h \in H}$, $X_h = \mathrm{Lin}\{1, t, t^2, \dots, t^n\}$, $h(n+1) = 1$, $n = 0, 1, \dots$ dello spazio $C[0, 1]$ non ammette proiezioni lineari che soddisfino alla condizione (K). In effetti se $\lambda_h = \inf \|p_h\|$, dove l'estremo inferiore è preso su tutte le proiezioni lineari limitate p_h di X su X_h, allora $\lambda_h \geq \log h / 8\sqrt{\pi}$, e di conseguenza $\lim_{h \to 0} \lambda_h = \infty$. Si osservi che l'approssimazione dello spazio $C[0, 1]$ data dai polinomi di Bernstein per mezzo del teorema di Weierstrass non soddisfa la condizione I).

Per formulazioni piú generali di fatti simili si veda Singer 1970.

Quando è data la famiglia di proiezioni $\{p_h\}_{h \in H}$, che soddisfi I) e II), possiamo definire la famiglia $\{X_h\}_{h \in H}$ di sottoinsiemi di X mediante la relazione $X_h = p_h X$, per ogni $h \in H$. Si dimostra che la famiglia $\{X_h, p_h\}_{h \in H}$ è un'approssimazione dello spazio X se le condizioni I), II), (K) sono soddisfatte e $\lim_{h \to 0} \|p_h z - z\| = 0$ per ogni z appartenente a un sottoinsieme arbitrario Z denso in X. Questa osservazione è spesso utile nelle applicazioni.

Esempio 1.

Sia $X = C[0, 1]$ lo spazio di tutte le funzioni reali continue sull'intervallo chiuso $[0, 1]$, con la norma $\|u\|_C = \sup_{t \in [0,1]} |u(t)|$ per ogni $u \in C[0, 1]$. Ponendo $H = [h | hn = 1, n = 1, 2, \dots]$,

$$s_{hj}(t) = f\left(\frac{t}{h} - j\right)$$

per $0 \leq t \leq 1$ $hn = 1$, $n = 1, 2, \dots$, $j = 0, 1, \dots, n$, dove

$$f(t) = \begin{cases} 1 - |t| & \text{se } |t| < 1 \\ 0 & \text{se } |t| \geq 1 \end{cases}$$

$$r^s_{hj}(u) = u(jh)$$

per ogni $u \in C[0, 1]$, $j = 0, 1, \dots, n$, $nh = 1$, $n = 1, 2, \dots$, troviamo che la famiglia $\{S_h, p^s_h\}_{h \in H}$ definita da

$$S_h = \mathrm{Lin}\{s_{h0}, s_{h1}, \dots, s_{hn}\}$$

e

$$p^s_h u = \sum_{j=0}^{n} r^s_{hj}(u) s_{hj}$$

per ogni $u \in C[0, 1]$ e $h \in H$ è l'approssimazione dello spazio $C[0, 1]$. Questo segue dalle relazioni $p^s_h p^s_h = p^s_h$ e $\|p^s_h\| < 1$. Il sistema $\{s_{hj}\}_{j=0,\, h \in H}^{n}$ è noto come la base di Schauder dello spazio $C[0, 1]$.

Le basi di Schauder sono intimamente collegate all'approssimazione mediante *splines*. Estendendo questo concetto agli spazi di funzioni di molte variabili otteniamo la cosiddetta approssimazione ad elementi finiti.

Esempio 2.

Prendiamo $X = C[0, 1]$ ed H come nell'esempio 1.

Definiamo l'insieme delle funzioni $\{w_{hj}\}_{j=0,\, h \in H}^{n}$ come segue:

$$w_{hj}(t) = \prod_{\substack{q=0 \\ q \neq j}}^{n} \frac{t - t_q}{t_j - t_q}$$

dove $0 \leq t_0 < t_1 < \dots < t_n \leq 1$, per $j = 0, 1, \dots, n$, $nh = 1$, $n = 1, 2, \dots$

La famiglia di funzionali $\{r^w_{hj}\}_{j=0,\, h \in H}^{n}$ è data da $r^w_{hj} u = u(t_j)$ per ogni $u \in C[0, 1]$ e j, h come sopra.

Consideriamo la famiglia $\{W_h, p^w_h\}_{h \in H}$ definita dalle relazioni

$$W_h = \mathrm{Lin}\{w_{h0}, w_{h1}, \dots, w_{hn}\}$$

per $nh = 1$, $n = 1, 2, \dots$,

$$p^w_h u = \sum_{j=0}^{n} r^w_{hj}(u) w_{hj},$$

per ogni $u \in C[0, 1]$. La funzione $p_n^w u$ è la ben nota interpolazione polinomiale di Lagrange della funzione u. Se la funzione ha tutte le derivate fino all'ordine n che sono continue nell'intervallo chiuso $[0, 1]$, allora

$$u(t) - p_n^w u(t) = \frac{1}{n!} u^{(n)}(\xi) \prod_{j=0}^{n} (t - t_j)$$

per ogni $t \in [0, 1]$ e $0 < \xi < 1$ con ξ dipendente da t.

Prendendo come Z l'insieme

$$Z = \left[u | u \in C^\infty[0, 1], \ \lim \frac{1}{n!} \|u^{(n)}\|_C = 0 \right]$$

vediamo che $\{W_h, p_h^w\}_{h \in H}$ è l'approssimazione dell'insieme Z nello spazio $C[0, 1]$. Osserviamo che in questo esempio la famiglia $\{p_h^w\}_{h \in H}$ non è uniformemente limitata in $C[0, 1]$.

Esempio 3.

Sia X lo spazio $L^q(0, 1)$ di tutte le funzioni che sono integrabili alla potenza q, $1 \leq q < \infty$. Questo è uno spazio normato con la norma definita da $\|u\|_{Lq} = \int_0^1 |u(t)|^q \, dt$.

L'approssimazione $\{L_h^q, p_h^L\}_{h \in H}$ è definita come segue:

$$H = [h | h(n+1) = 1, \ n = 0, 1, \ldots],$$
$$L_h^q = \mathrm{Lin}\{l_{h0}, l_{h1}, \ldots, l_{hn}\}$$

per $h(n+1) = 1$, $h \in H$,

$$p_h^L u = \sum_{j=0}^{n} r_{hj}^L(u) l_{hj}$$

per ogni $u \in L^q(0, 1)$; dove

$$l_{hj}(t) = \chi\left(\frac{t}{h} - j\right), \text{ per } t \in (0, 1), \ \chi(t) = \begin{cases} 1 \text{ se } t \in (0, 1) \\ 0 \text{ se } t \notin (0, 1) \end{cases}$$

$$r_{hj}^L u = \frac{1}{h} \int_0^1 u(t) l_{hj}(t) \, dt$$

per ogni $u \in L^q(0, 1)$, $j = 0, 1, \ldots, n$, $h(n+1) = 1$, $h \in H$.

Esempio 4.

È facile dimostrare che se la famiglia $\{p_h\}_{h \in H}$ definita dall'approssimazione $\{X_h, p_h\}_{h \in H}$ dello spazio di Banach X ha la forma seguente

$$p_h x = \sum_{j=1}^{n} r_{hj}(x) x_{hj},$$

dove $\{x_{hj}\}_{j=1}^n$ è la base in X_h e $\{r_{hj}\}_{j=1}^n$ è un insieme biortonormale di funzionali lineari, allora l'applicazione duale p_h^* che applica lo spazio X^* di tutti i funzionali lineari di X in $X_h^* = \mathrm{Lin}\{r_{h0}, r_{h1}, \ldots, r_{hn}\}$ è data dalla formula

$$p_h^* y = \sum_{j=1}^{n} y(x_{hj}) r_{hj}$$

per ogni $y \in X^*$. Se la famiglia $\{X_h, p_h\}_{h \in H}$ è l'approssimazione dello spazio X, allora la famiglia $\{X_h^*, p_h^*\}_{h \in H}$, con ipotesi addizionali, è un'approssimazione dello spazio X^*. Questo può usarsi per una approssimazione dei funzionali.

Consideriamo lo spazio $C[0, 1]$ e la sua approssimazione definita nell'esempio 2. Il funzionale $Iu = \int_0^1 u(t) \, dt$ è lineare e definito su $C[0, 1]$. Di conseguenza si può approssimare il funzionale con la formula

$$p_n^w Iu = \sum_{j=0}^{n} I(w_{hj}) r_{hj}^w(u) = \sum_{j=0}^{n} \left[\int_0^1 w_{hj}(t) \, dt \right] u(t_j)$$

che è la ben nota formula di approssimazione di Newton-Cotes.

La relazione

$$|Iu - p_h^w Iu| = \left| \int_0^1 u(t) \, dt - \sum_{j=0}^{n} \left[\int_0^1 w_{hj}(t) \, dt \right] u(t_j) \right| \leq$$
$$\leq \|u^{(n)}\|_C \left[\int_0^1 \frac{1}{n!} \prod_{j=0}^{n} |t - t_j| \, dt \right] \leq \frac{1}{n!} \|u^{(n)}\|_C$$

fornisce l'errore della formula d'integrazione di Newton-Cotes sull'intervallo $[0, 1]$ [cfr. Hildebrand 1974].

3. *Approssimazione ottimale negli spazi di Banach.*

Se $\{X_h\}_{h \in H}$ è un approssimante di dimensione finita dello spazio di Banach X, cioè per ogni $h \in H$, X_h è un sottospazio di X di dimensione finita, allora esiste un'approssimazione ottimale dello spazio X.

Questo significa che esiste una famiglia di funzioni $\{\mathring{p}_h\}_{h \in H}$ tale che $\mathring{p}_h : X \to X_h$ e $\|\mathring{p}_h x - x\| = \inf_{v \in X_h} \|x - v\|$, per ogni $x \in X$ ed $h \in H$.

In generale, noi non conosciamo abbastanza gli elementi dell'approssimazione ottimale per determinare le funzioni $\mathring{p}_h$.

È possibile, per alcuni spazi, la costruzione di algoritmi che determinano l'approssimazione ottimale.

Si consideri dapprima lo spazio $C(Q)$ di tutte le funzioni reali continue nell'insieme compatto Q.

Il sistema di funzioni $u_1, \ldots, u_n$, $u_j \in C(Q)$, per $j = 1, \ldots, n$, è detto il sistema di Čebyšev, in $C(Q)$ se comunque scelti n punti distinti, $t_1, \ldots, t_n \in Q$, $\det(u_i(t_j))_{i, j=1, \ldots, n} \neq 0$.

L'approssimazione ottimale in $C(Q)$ è caratterizzata dal seguente teorema [cfr. Singer 1974]:

TEOREMA. *Se $\{X_h\}_{h\in H}$ è l'approssimante di $C(Q)$ definito nel modo seguente: $X_h = \mathrm{Lin}\{u_{h1}, \ldots, u_{hn}\}$ per $hn = 1$, $h \in H = [h|hn = 1, n = 1, 2, \ldots]$ e $u_{h1}, \ldots, u_{hn}$ è il sistema di Čebišev in $C(Q)$, allora $v_h \in X_h$ è un elemento di un'approssimazione ottimale di $u \in C(Q) \setminus X_h$ se e solo se esistono $n+1$ punti distinti $t_1, \ldots, t_{n+1} \in Q$ tali che*

$$D = \det \begin{vmatrix} u_{h1}(t_1), & \ldots, & u_{h1}(t_{n+1}) \\ \cdot & \cdot & \cdot \\ u_{hn}(t_1), & \ldots, & u_{hn}(t_{n+1}) \\ u(t_1), & \ldots, & u(t_{n+1}) \end{vmatrix} \neq 0$$

e

$$u(t_j) - v_h(t_j) = \left(\operatorname{sign} \frac{D_j}{D}\right) \sup_{t\in Q} |u(t) - v_h(t)| \qquad \textit{per } j = 1, \ldots, n+1$$

dove D_j è il cofattore di $u(t_j)$ in D.

Quando si prende come compatto Q l'intervallo $[a, b]$, allora con le ipotesi del teorema stabilito sopra, si ottiene il seguente corollario:

COROLLARIO. $v_h \in X_h$ è un elemento dell'approssimazione ottimale di $u \in C[a, b] \setminus X_h$ se e solo se esistono $n+1$ punti distinti $t_1, t_2, \ldots, t_{n+1}$ dell'intervallo $[a, b]$ nei quali la funzione $u(t) - v_h(t)$ ha il valore $\sup_{t\in[a,b]} |u(t) - v_h(t)|$ con segni alternati, cioè con segni opposti in ogni punto t_j, t_{j+1}.

Questo risultato è noto come il «teorema dell'alternanza» di P. L. Čebyšev e fornisce la base per gli algoritmi numerici che determinano i polinomi dell'approssimazione ottimale [cfr. Ramez 1957 e Stiefel 1960].

Sia V un sottospazio dello spazio lineare normato X. Come conseguenza del teorema di Hahn-Banach otteniamo la seguente caratterizzazione degli elementi dell'approssimazione ottimale: v_0 è un elemento dell'approssimazione ottimale di $x \in X \setminus \bar{V}$, cioè $\|v_0 - x\| = \inf_{v\in V} \|v - x\|$ se e solo se esiste un funzionale lineare f_x di X tale che $\|f_x\| = 1$, $f_x(x - v_0) = \|x - v_0\|$ e $f_x(v) = 0$ per ogni $v \in V$.

La condizione posta sopra è l'estensione della condizione di ortogonalità nello spazio di Hilbert. In effetti, se X è uno spazio di Hilbert, con prodotto scalare denotato da $(\ ,\ )$, allora, mediante il teorema di Riesz, è possibile dimostrare che esiste esattamente un funzionale lineare e continuo f su X, tale che per il dato elemento $x \in X$, $fx = \|x\|$ e $\|f\| = 1$. Questo funzionale è definito dalla relazione $fy = \left(y, \dfrac{x}{\|x\|}\right)$.

Di conseguenza, se V è un sottospazio dello spazio di Hilbert X, allora v_0 è la migliore approssimazione di $u \in X \setminus \bar{V}$, cioè $\|v_0 - u\| = \inf_{v\in V} \|v - u\|$ se e solo se $(v, u - v_0) = 0$ per ogni $v \in V$. L'ultima equazione significa che l'elemento $u - v_0$ è ortogonale a tutti gli elementi del sottospazio V.

L'elemento v_0 è unico. In realtà, se esiste un altro elemento $w_0 \in V$ tale che $(v, u - w_0) = 0$ per ogni $v \in V$, allora $(v, w_0 - v_0) = 0$ per $v \in V$ e prendendo $v = w_0 - v_0 \in V$ si trova $0 = (w_0 - v_0, w_0 - v_0) = \|w_0 - v_0\|^2$, cioè $w_0 = v_0$.

Ora è possibile trovare l'approssimazione ottimale $\{X_h, \mathring{p}_h\}_{h\in H}$ dello spazio di Hilbert X. Sia l'approssimante $\{X_h\}_{h\in H}$ dato nella forma $X_h = \mathrm{Lin}\{x_{h1}, \ldots, x_{hn}\}$ per $hn = 1$, $h \in H = [h|nh = 1, n = 1, 2, \ldots]$. Allora esiste esattamente una base $y_{h1}, \ldots, y_{hn}$ nel sottospazio X_h che è biortogonale al sistema $x_{h1}, \ldots, x_{hn}$, cioè $(y_{hk}, x_{hj}) = \delta_{kj}$ per $k, j = 1, \ldots, n$. Questa base è data dalle equazioni:

$$y_{hk} = \sum_{j=1}^{n} a_{kj}^h x_{hj}$$

per $k = 1, \ldots, n$, dove gli scalari a_{kj}^h sono determinati dal sistema di equazioni algebriche lineari

$$\sum_{j=0}^{n} a_{kj}^h (x_{hj}, x_{hm}) = \delta_{km}$$

per $k, m = 1, \ldots, n$. Questo significa che la matrice $(a_{kj}^h)_{k,j=1}^n$ è l'inversa della matrice di Gram $(x_{hi}, x_{hj})_{i,j=1}^n$ del sistema di elementi $x_{h1}, \ldots, x_{hn}$ che sono linearmente indipendenti, perciò la matrice (a_{kj}^h) esiste ed è unica.

Definendo $\mathring{p}_h$ con la relazione

$$\mathring{p}_h u = \sum_{j=1}^{n} (u, y_{hj}) x_{hj}$$

per ogni $u \in X$, $h \in H$, $hn = 1$, si verifica facilmente che $(v, u - \mathring{p}_h u) = 0$ per ogni $v \in X_h$ e $u \in X$, il che dimostra che la famiglia $\{X_h, \mathring{p}_h\}_{h\in H}$ è l'approssimazione ottimale dello spazio di Hilbert X.

Si osservi, per concludere, che se il sistema $x_{h1}, \ldots, x_{hn}$ è ortonormale*, cioè se $(x_{hj}, x_{hk}) = \delta_{jk}$, per $j, k = 1, \ldots, n$, allora $y_{hj} = x_{hj}$ per $j = 1, \ldots, n$ e $\mathring{p}_h u = \sum_{j=0}^{n} (u, x_{hj}) x_{hj}$, per tutti gli $u \in X$ ed $h \in H$.

4. *Approssimazione degli operatori.*

Siano X ed Y spazi di Banach, e sia $D(A) \subset X$ il dominio di un operatore continuo (in generale non lineare) A, $A : D(A) \to Y$. Assumiamo che $D(A)$ sia aperto in X e le famiglie $\{X_h, p_h^x\}_{h\in H}$ $\{Y_h, p_h^y\}_{h\in H}$ siano approssimazioni degli spazi X ed Y che soddisfano la condizione (K) incontrata in precedenza.

La famiglia di operatori $\{A_h\}_{h\in H}$ è detta un'approssimazione dell'operatore A se e solo se:

* I sistemi ortonormali sono stati studiati in diversi spazi di Hilbert; per i polinomi ortogonali cfr. Szegö 1959, in particolare si cerchino i polinomi di Čebyšev, Hermite, Jacobi, ecc. Cfr. anche, per le serie di Fourier, Yosida 1974.

a) per ogni $h \in H$, $A_h : D_h(A) \to Y_h$, dove $D_h(A) = D(A) \cap X_h$;
b) per ogni $x \in D(A)$ e ogni $\varepsilon > 0$ esiste un numero positivo h_0 tale che per ogni $h \in H$, $h < h_0$ si abbia

$$\|A_h(p_h^x x) - A(x)\|_Y < \varepsilon.$$

Si osservi che la famiglia $\{A_h\}_{h \in H}$ dove

$$A_h(x_h) = p_h^y A(x_h),$$

per ogni $x_h \in D_h(A)$ e $h \in H$, è una approssimazione di A. Per verificare quest'asserzione si osserva dapprima che la condizione *a*) è soddisfatta per la definizione di A_h. Proviamo ora che è soddisfatta la condizione *b*).

Poiché l'insieme $D(A)$ è aperto, per ogni $x \in D(A)$ esiste un numero positivo h_1 tale che per ogni $h \in H$, $h \leq h_1$, $p_h^x x \in D_h(A) = D(A) \cap X_h$, poiché $\{X_h, p_h^x\}_{h \in H}$ è un'approssimazione di X. Assumendo la continuità di A si vede che per ogni $x \in D(A)$ e ogni numero positivo ε esiste un numero positivo h_2 tale che per ogni $h \in H$, $h \leq h_2$

$$\|A(p_h^x x) - A(x)\|_Y < \frac{\varepsilon}{2K},$$

dove $\|p_h^y\| < K$. D'altronde, per ogni $x \in D(A)$ esiste un numero positivo h_3 tale che per ogni $h \in H$, $h < h_3$, $\|p_h^y A(x) - A(x)\|_Y < \varepsilon/2$, poiché la famiglia $\{Y_h, p_h\}_{h \in H}$ è un'approssimazione di Y.

Infine, per ogni $x \in D(A)$, per ogni $\varepsilon > 0$ e $h \in H$, $h \leq \min(h_1, h_2, h_3)$

$$\begin{aligned}\|p_h^y A(p_h^x x) - A(x)\|_Y &\leq \|p_h^y A(p_h^x x) - p_h^y A(x)\|_Y + \|p_h^y A(x) - A(x)\|_Y \leq \\ &\leq \|p_h^y\| \, \|A(p_h^x x) - A(x)\|_Y + \|p_h^y A(x) - A(x)\|_Y \\ &< K \frac{\varepsilon}{2K} + \frac{\varepsilon}{2} = \varepsilon\end{aligned}$$

che prova che la condizione *b*) è soddisfatta.

Esempio 5.

L'operatore $\mathcal{J}$, $\mathcal{J}u = \int_0^1 u(t)\, dt$ applica lo spazio $C[0, 1]$ nello spazio R dei numeri reali. Prendiamo come approssimazione di $C[0, 1]$ $\{S_h, p_h^s\}_{h \in H}$ descritta nell'esempio 1, mentre come approssimazione di R possiamo prendere R stesso, cioè la famiglia costante $\{R, I\}_{h \in H}$. Possiamo prendere come approssimazione $\{\mathcal{J}_h\}_{h \in H}$ dell'operatore $\mathcal{J}$ quella che è definita dalle approssimazioni dello spazio $C[0, 1]$ e da R. Allora

$$\mathcal{J}_h p_h^s u = \mathcal{J} p_h^s u = \sum_{j=0}^{n} u(jh) \mathcal{J} s_{hj}$$

per ogni $u \in C[0, 1]$ e $h \in H$.

Poiché $\mathcal{J} s_{hj} = \int_0^1 f\left(\frac{t}{h} - j\right) dt = h \int_j^{n-j} f(z)\, dz = \begin{cases} \frac{h}{2} & \text{per } j = 0, n \\ h & \text{per } 1 \leq j \leq n-1 \end{cases}$

si ha

$$\mathcal{J}_h p_h^s u = \frac{h}{2} \left[u(0) + \sum_{j=1}^{n-1} u(jh) + u(1) \right].$$

Questa è la ben nota regola per l'approssimazione mediante trapezi generalizzata.

Esempio 6.

L'operatore D, $Du = du/dt$ applica lo spazio $C^1[0, 1]$ di tutte le funzioni differenziabili nell'intervallo chiuso $[0, 1]$ nello spazio $C[0, 1]$.

Definiamo l'approssimazione dello spazio $C^1[0, 1]$ come la famiglia $\{C_h, p_h^c\}_{h \in H}$ nel modo seguente:

$$\begin{aligned} H &= [h \mid hn = 1,\ n = 1, 2, \ldots] \\ C_h &= \operatorname{Lin}\{c_{h0}, \ldots, c_{hn}\} && \text{per } nh = 1,\ h \in H \\ p_h^c u &= \sum_{j=0}^{n} u(jh) c_{hj} && \text{per ogni } u \in C^1[0, 1],\ hn = 1,\ h \in H \end{aligned}$$

dove

$$c_{hj}(t) = \begin{cases} g\left(j - \frac{t}{h}\right) & \text{per } j = 0, \ldots, n-1 \\ g\left(n - \frac{t}{h}\right) + g\left(\frac{t}{h} - n\right) & \text{per } j = n \end{cases}$$

e

$$g(t) = \begin{cases} 0 & \text{per } t \notin (-1, 2) \\ \frac{1}{2}(t+1)^2 & \text{per } -1 \leq t \leq 0 \\ -t^2 + t + \frac{1}{2} & \text{per } 0 < t \leq 1 \\ \frac{1}{2}(t-2)^2 & \text{per } 1 \leq t \leq 2 \end{cases}$$

Quest'approssimazione non soddisfa la condizione 1) richiesta in precedenza cioè p_h^c non è un operatore proiettivo. Tuttavia la famiglia di operatori $\{p_h^c\}_{h \in H}$ è uniformemente limitata e $\lim_{h \to 0} p_h^c = I$, il che ci permette di usare un metodo generale per trovare un'approssimazione dell'operazione D formulata all'inizio di questo paragrafo: si veda la dimostrazione di *b*).

Come approssimazione dello spazio $C[0, 1]$ prendiamo la famiglia defi-

nita nell'esempio 1 $\{S_h, p_h^s\}_{h\in H}$. Allora la famiglia $\{D_h\}_{h\in H}$, che è un'approssimazione dell'operatore D, può essere definita nel modo seguente:

$$D_h p_h^c u = p_h^s D p_h^c u = \sum_{j=0}^{n} (D p_h^c u)(jh)\, s_{hj}$$

per $u\in C^1[0, 1]$, $nh=1$, $h\in H$. Poiché

$$(D p_h^c u)(jh) = \sum_{k=0}^{n} u(kh)(Dc_{hk})(jh)$$

e

$$Dc_{hk}(jh) = \begin{cases} -\dfrac{1}{h} g'(k-j) = \dfrac{1}{h}[\delta_{k,\,j+1} - \delta_{k,\,j}], & \text{per } k=0, \ldots, n-1 \\[2ex] \dfrac{1}{h}[g'(j-k) - g'(k-j)] = \dfrac{1}{h}\,\delta_{n,\,j+1} & \text{per } k=n \end{cases}$$

otteniamo

$$D_h p_h^c u = \sum_{j=0}^{n} \frac{u((j+1)h) - u(jh)}{h}\, s_{hj}$$

per $u\in C^1[0, 1]$.

Questa è la ben nota approssimazione con le differenze finite della derivata D. Per una costruzione piú generale si veda Aubin 1972.

Osservazione. Tutte le nostre considerazioni sono basate sulla nozione di approssimazione interna, cioè l'approssimazione di un dato spazio mediante i suoi sottoinsiemi. È possibile tuttavia, e talvolta necessario, usare approssimazioni di spazi che contengono lo spazio dato (approssimazioni esterne). Per ulteriori dettagli si veda Aubin 1972.

5. *Approssimazione di equazioni operatoriali.*

Sia A un operatore continuo, $A : D(A) \to Y$, $D(A) \subset X$. Considereremo il seguente problema:

PROBLEMA 1. Per un dato $y_0 \in Y$ trovare $x_0 \in D(A)$ tale che $A(x_0) = y_0$.

Si supponga che il problema sia ben posto, cioè che per ogni numero positivo ε esista un numero positivo δ tale che per ogni $\tilde{y}\in Y$, con $\|y-\tilde{y}\|_Y < \delta$, l'equazione $A\tilde{x} = \tilde{y}$ ha una soluzione $\tilde{x}\in D(A)$ che soddisfa la disuguaglianza $\|x-\tilde{x}\|_X < \varepsilon$.

In generale non si può trovare la soluzione del problema esattamente, e ricerchiamo perciò la sua approssimazione.

La famiglia $\{x_h\}_{h\in H}$ tale che per ogni $h\in H$, $x_h \in D(A)\cap X_h$ e $\lim_{h\to 0} \|x - x_h\|_X = 0$, è detta un'approssimazione della soluzione del problema, purché $\{X_h, p_h\}_{h\in H}$ sia un'approssimazione dello spazio X.

Si vuole trovare questa approssimazione della soluzione risolvendo la seguente famiglia di problemi di dimensione finita:

PROBLEMA 2. Per ogni $h\in H$ trovare $x_h \in D_h(A) = D(A)\cap X_h$ che soddisfa l'equazione

$$p_h^y A(x_h) = p_h^y y.$$

L'esistenza di una soluzione del problema dipende in generale da un operatore A e dalle proprietà delle approssimazioni $\{X_h, p_h^x\}_{h\in H}$ e $\{Y_h, p_h^y\}_{h\in H}$ di X e Y. Supponendo che esista una soluzione, si possono dare alcune condizioni sufficienti che assicurano che è un'approssimazione della soluzione del problema 1.

Si definisce la famiglia di funzionali $\{S_h(A, x, \rho)\}$:

$$S_h(A, x, \rho) = \sup_{\substack{z\in D_h(A) \\ \|z-x\|_X<\rho}} \frac{\|z - p_h^x x\|_X}{\|p_h^y A(z) - p_h^y A(p_h^x x)\|_Y}$$

per ogni $h\in H$, $x\in D(A)$ ed ogni numero reale positivo ρ.

Dalla definizione di S_h si ottiene dunque:

$$\|x_h - p_h^x x\|_X \le S_h(A, x, \rho)\, \|p_h^y A(x_h) - p_h^y A(p_h^x x)\|_Y .$$

Di conseguenza:

$$\begin{aligned} \|x_h - x\|_X &\le \|x_h - p_h^x x\|_X + \|p_h^x x - x\|_X \le \\ &\le S_h(A, x, \rho)\, \|p_h^y A(x_h) - p_h^y A(p_h^x x)\|_Y + e_h(x) = \\ &= S_h(A, x, \rho)\, \|p_h^y A(x) - p_h^y A(p_h^x x)\|_Y + e_h(x), \end{aligned}$$

poiché x è una soluzione del problema 1 e $\{x_h\}_{h\in H}$ una soluzione del problema 2.

Noi assumiamo che la famiglia $S_h(A, x, \rho)$ sia uniformemente limitata rispetto ad h, cioè che esista un numero positivo h_0 tale che per ogni $h\in H$, $h<h_0$, $S_h(A, x, \rho) \le S(A, x, \rho) < \infty$. L'ultima condizione è detta di stabilità locale di Lax-Richtmyer [cfr. Aubin 1972 e Richtmyer e Morton 1967]. Da queste ipotesi segue che $\lim_{h\to 0} \|x_h - x\|_X = 0$, che dimostra che $\{x_h\}_{h\in H}$ è un'approssimazione della soluzione x del problema 1.

Si osservi infine come il problema 2 sia puramente algebrico. Infatti, poiché

$$p_h^y y = \sum_{j=0}^{n} r_{hj}^y(y)\, y_{hj}$$

$Y_h = \mathrm{Lin}\{y_{h0}, \ldots, y_{hn}\}$ e per ogni $x_h \in X_h = \mathrm{Lin}\{x_{h0}, \ldots, x_{hn}\}$ esistono dei numeri $t_0, \ldots, t_n$ tali che

$$x_h = \sum_{j=0}^{n} t_j x_{hj},$$

allora il problema 2 può essere formulato nel modo seguente: trovare dei numeri $t_0, \ldots, t_n$, che soddisfino il sistema di relazioni

$$r^y_{hj} A\left(\sum_{j=0}^{n} t_j x_{hj}\right) = r^y_{hk} y$$

per $k=0, \ldots, n$,

$$\sum_{j=0}^{n} t_j x_{hj} \in D_n(A).$$

Esempio 7.

Si consideri l'equazione integrale:

$$Au = u(t) + \int_0^1 K(t, s) u(s)\, ds = f(t),$$

per $u \in C[0, 1] = X$. Qui A applica X su X e prendendo $\{S_h, p^s_h\}_{h \in H}$ come abbiamo fatto nell'esempio 1, come approssimazione di $C[0, 1]$, si trova che il problema approssimato ha la forma: trovare dei numeri $u_{h0}, \ldots, u_{hn}$ che soddisfano il sistema di equazioni algebriche lineari

$$\sum_{j=0}^{n} m^h_{kj} u_{hj} = f(kh)$$

per $k=0, 1, \ldots, n$, dove

$$m^h_{kj} = \delta_{kj} + \int_0^1 K(kh, t) s_{hj}(t)\, dt,$$

per $k, j = 0, 1, \ldots, n$ e $h \in H$.

Se

$$\sup_{0 \le t \le 1} \int_0^1 |K(t, s)|\, ds < 1$$

allora la matrice $M_h = (m^h_{kj})_{kj=0}^{n}$ non è singolare poiché

$$|I - M_h|_\infty = \max_{0 \le k \le n} \int_0^1 |K(kh, t)|\, dt < 1.$$

Quindi il sistema di equazioni discusse sopra ha un'unica soluzione.

Inoltre si ha

$$S_h(A, u, \rho) \le \left[1 - \sup_{0 \le t \le 1} \int_0^1 |K(t, s)|\, ds\right]^{-1} = S < \infty$$

e la famiglia di problemi approssimati è globalmente stabile nel senso di Lax-Richtmyer. Ciò dimostra che la famiglia $\{u_h\}_{h \in H}$ dove $u_h = \sum_{j=0}^{n} u_{hj} s_{hj}$ è un'approssimazione della soluzione dell'equazione integrale considerata.

Esempio 8.

Si consideri il seguente problema con valori iniziali: trovare $u \in C^1[0, 1]$ tale che per $0 < t < 1$

$$\frac{du}{dt} - f(t, u) = 0$$

$$u(0) = a,$$

dove f è una funzione continua.

Utilizzando i risultati dell'esempio 6 otteniamo

$$p^s_h A p^c_h u(t) = \sum_{j=0}^{n-1} \left[\frac{u_{j+1} - u_j}{h} - f(jh, u_j)\right] s_{hj}$$

per $0 \le t \le 1 - h$, poiché $f(jh, (p^c_h u)(jh)) = f(jh, u_j)$, dove $u_j = u(jh)$.

Il problema algebrico corrispondente ha la forma

$$u_0 = a$$

$$u_{j+1} = u_j + hf(jh, u_j)$$

per $j = 0, 1, \ldots, n-1$, e dunque può essere risolto.

Se la funzione f è lipschitziana rispetto alla seconda variabile con costante L, cioè

$$|f(t, u) - f(t, v)| \le L|u - v|$$

allora per il funzionale S_h abbiamo la stima

$$S_h \le \frac{1}{L}(e^L - 1).$$

Questa disuguaglianza implica che la famiglia

$$\{u_h\}_{h \in H} u_h = \sum_{j=0}^{n} u_j s_{hj}$$

è un'approssimazione della soluzione del problema ai valori iniziali considerato.

Abbiamo dato qui solamente esempi molto primitivi delle soluzioni approssimate delle equazioni con operatori. Un'esposizione molto buona e particolareggiata dei problemi relativi per le equazioni differenziali ordinarie può essere trovata in Henrici 1964; per le equazioni alle derivate parziali si vedano Aubin 1972, Richtmyer e Morton 1967, Babuška e Aziz 1973.

6. *Processi iterativi. Approssimazioni generate.*

Nel paragrafo precedente abbiamo considerato un'equazione operatoriale in uno spazio di dimensione infinita. Abbiamo descritto un procedimento generale che riduce un dato problema di dimensione infinita ad una famiglia di

problemi di dimensione finita. Qui discuteremo un altro modo per costruire un'approssimazione di soluzioni di un'equazione operatoriale.

Siano X, Y spazi lineari normati e sia f un'applicazione da $U \subset X$ su Y. Per un dato elemento $y \in Y$ si consideri l'equazione $f(x) = y$, sotto l'ipotesi: esiste un insieme aperto convesso $V \subset U$ tale che l'equazione considerata ha un'unica soluzione in V.

Si supponga che esista una data sequenza di operatori lineari invertibili $\{A_j\}_{j=1}^{\infty}$ tale che per ogni j, $j = 1, 2, \ldots$, $A_j : f(U) \to X$. Definendo la sequenza di funzioni $\{F_j\}_{j=1}^{\infty}$ con la formula $F_j(x) = x + A_j[f(x) - y]$ per ogni $x \in U$ e $j = 1, 2, \ldots$, si può vedere che per ogni j, $j = 1, 2, \ldots$, l'equazione $F_j(x) = x$ è equivalente all'equazione $f(x) = y$, poiché esiste A_j^{-1}.

Sia x_0 l'unica soluzione dell'equazione considerata nell'insieme V. Supponiamo che esistano due numeri reali positivi r ed L tali che l'intorno aperto $K(x_0, r)$, $K(x_0, r) = [x | x \in X, \|x - x_0\| < r]$, sia contenuto in V, e per L, $0 < L < 1$, la disuguaglianza

$$\text{(L)} \qquad \|F_j(x) - x_0\| = \|F_j(x) - F_j(x_0)\| \leq L\|x - x_0\|$$

sia soddisfatta per tutti gli $x \in K(x_0, r)$ e $j = 1, 2, \ldots$ Definiamo una famiglia $\{X_h, p_h^x\}_{h \in H}$ come segue:

$$H = [h | nh = 1;\ n = 1, 2, \ldots]$$
$$X_1 = K(x_0, r),\ X_{1/(n+1)} = F_h(X_{1/n})$$

per $n = 1, 2, \ldots$,

$$p_h^x(x_0) = F_n F_{n-1} \ldots F_1(x),$$

dove x è un elemento fissato da X_1 e $nh = 1$, $h \in H$.

Per dimostrare che la famiglia $\{X_h p_h^x\}_{h \in H}$ è un'approssimazione dell'elemento x_0, osserviamo dapprima che

$$\|p_{1/n}^x(x_0) - x_0\| = \|F_n(p_{1/(n-1)}^x(x_0)) - x_0\| = \|F_n(p_{1/(n-1)}^x(x_0)) - F_n(x_0)\| \leq$$
$$\leq L\|p_{1/(n-1)}^x(x_0) - x_0\| \leq \ldots \leq L^n\|x - x_0\| < r$$

per ogni $x \in X_1$. Questo significa che $p_{(1/n)}^x(x_0) \in X_1$, per cui X_h e p_h^x sono ben definiti per ogni $h \in H$. Inoltre, per ogni $h \in H$ ed $x \in X_1$, $p_h^x(x_0) \in X_h$ e $\lim_{h \to 0} \|p_h^x(x_0) - x_0\| = 0$. Questo dimostra che la famiglia $\{X_h, p_h^x\}_{h \in H}$ è un'approssimazione dell'elemento x_0.

Facciamo ora alcune osservazioni che concernono l'approssimazione discussa.

1) Per prima cosa si noti che l'approssimazione considerata in questo paragrafo differisce da quelle discusse in precedenza. Gli insiemi X_h e le applicazioni p_h^x non sono date a priori, ma sono formati con un procedimento iterativo, cioè l'approssimazione è generata.

2) Poiché una successione $\{p_{1/n}^x(x_0)\}_{n=1}^{\infty}$ converge ad x_0 per ogni $x \in K(x_0, r)$ allora una successione $\{y_n\}_{n=1}^{\infty}$ definita dalle relazioni $y_1 = x$, $y_k = F_{k-1}(y_{k-1})$, per $k = 2, 3, \ldots$, converge pure ad x_0, poiché $y_k = p_{1/(k-1)}^x x_0$.

Le formule che determinano la successione $\{y_k\}_{k=1}^{\infty}$ formano il ben noto metodo iterativo per risolvere l'equazione $f(x) = y$.

3) Molto difficili, ma in generale impossibili da evitarsi, i problemi nel costruire le approssimazioni considerate in questo paragrafo sono connessi con la determinazione di un opportuno insieme X_1 e di una opportuna successione $\{A_j\}_{j=1}^{\infty}$ di operatori che generano una convergenza. Considereremo qui questi problemi in due casi particolari.

a) Supponiamo che $A_j = A$ per $j = 1, 2, \ldots$ Allora $F_j(x) = F(x) = x + A[f(x) - y]$ per ogni j ed $x \in U$. Sia f differenziabile nel senso di Fréchet [cfr. Kantorovich e Akilov 1964] nel punto x_0, e $[(d/dx)f(x_0)]^{-1}$ esista e sia limitata. Applicando il teorema del valor medio abbiamo per la successione $\{y_k\}_{k=1}^{\infty}$ definita sopra al punto 2 la stima seguente:

$$\|y_{k+1} - x_0\| = \|F(y_k) - F(x_0)\| \leq \sup \left\| \frac{d}{dx} F(z) \right\| \|y_k - x_0\| =$$
$$= \sup \left\| I + A \frac{d}{dx} f(z) \right\| \|y_k - x_0\|,$$

dove I è l'operatore identico su X e l'estremo superiore è preso su tutti gli z della forma $z = ty_k + (1 - t)x_0$, $0 \leq t \leq 1$.

Si può dimostrare che la successione $\{y_k\}_{k=1}^{\infty}$ converge ad x_0 in qualche intorno sferico $K(x_0, r) \subset V$, se l'operatore A è abbastanza prossimo (in norma) all'operatore lineare

$$\left[\frac{d}{dx} f(x_0)\right]^{-1}.$$

Quando la funzione F soddisfa una condizione di Lipschitz allora, per il teorema del punto fisso di Banach-Cacciopoli, si può dimostrare l'esistenza e l'unicità della soluzione x_0 della equazione $F(x) = x$ ($f(x) = y$) negli spazi di Banach.

b) Un'altra classe importante di approssimazioni di una soluzione dell'equazione considerata può essere ottenuta supponendo:

$$A_j = -\left[\frac{d}{dx} f(p_{1/j}^x x_0)\right]^{-1}$$

per $j = 1, 2, \ldots$ Un processo iterativo $y_1 = x$, $y_{j+1} = F_j(y_j)$ per $j = 1, 2, \ldots$ ottenuto mediante tale scelta della successione $\{A_j\}_{j=1}^{\infty}$ è il ben noto metodo di Newton-Kantorovich per risolvere la equazione $f(x) = y$ in uno spazio di Banach [cfr. Dieudonné 1969]. [K. M. e A. W.].

Aubin, J. P.
1972 *Approximation of Elliptic Boundary-Value Problems*, Wiley-Interscience, New York.

Babuška, I., e Aziz, A. K.
1973 *Survey Lectures on the Mathematical Foundations of the Finite Element Method*, in A. K. Aziz (a cura di), *The Mathematical Foundations of the Finite Element Method with Applications to Partial Differential Equations*, Academic Press, New York.

Carnot, L.-N.-M.
1797 *Réflexions sur la métaphisique du calcul infinitésimal*, Paris (trad. it. Bolzani, Pavia 1803).
Dieudonné, J.
1969 *Foundations of Modern Analysis*, Academic Press, New York.
Farrington, B.
1947 *Head and Hand in Ancient Greece*, Watts, London (trad. it. Feltrinelli, Milano 1976).
Galilei, G.
1638 *Discorsi e dimostrazioni matematiche intorno a due nuove scienze*, Elzevier, Leida; ed. Boringhieri, Torino 1958.
Hegel, G. W. F.
1812 *Wissenschaft der Logik*, Schrag, Nürnberg 1812-13 (trad. it. Laterza, Bari 1968²).
Henrici, P.
1964 *Discrete Variable Methods*, in *Ordinary Differential Equations*, Wiley, New York.
Hildebrand, F. B.
1974 *Introduction to Numerical Analysis*, McGraw-Hill, New York.
Kantorovich, L. V., e Akilov, G. P.
1964 *Functional Analysis in Normed Spaces*, Pergamon Press, Oxford.
Koyré, A.
1961 *Du monde de l'« à-peu-près » à l'univers de la précision*, in *Etudes d'histoire de la pensée philosophique*, Colin, Paris (trad. it. Einaudi, Torino 1967).
Ramez, E.
1957 [Metodi generali di calcolo per l'approssimazione di Čebyšev. Problemi con parametri reali a ingresso lineare], Izdat. Akad. Nauk Ssr, Kiev (in russo).
Richtmyer, R. D., e Morton, K. W.
1967 *Difference Methods for Initial-Value Problems*, Wiley-Interscience, New York.
Rossi, P.
1976 *I filosofi e le macchine (1400-1700)*, Feltrinelli, Milano 1976².
Singer, I.
1970 *Best Approximation in Normed Linear Spaces by Elements of Linear Subspaces*, Springer, Berlin.
Stiefel, E.
1960 *Note on Jordan elimination, linear programming and Tschebyscheff approximation*, in « Numerical Mathematics », n. 2, pp. 1-17.
Szegö, G.
1959 *Orthogonal polynomials*, American Mathematical Society, New York.
Yosida, K.
1974 *Functional Analysis*, Springer, Berlin.

L'elevarsi dell'approssimazione da semplice esigenza del **calcolo** (e della **misura**) a concetto è intimamente legato al sorgere della **scienza** moderna. Al concetto di approssimazione è anche strettamente connessa l'origine del calcolo infinitesimale (cfr. **differenziale, infinitesimale**). I successivi sviluppi del concetto di approssimazione all'interno della matematica, di pari passo con il progressivo astrarsi e generalizzarsi di essa (cfr. **matematiche, strutture matematiche**), conducono ad una riformulazione del concetto stesso in termini sempre piú sofisticati e specifici. Cosí tutta la seconda parte dell'articolo che precede tratta a titolo esemplificativo di un problema importante ma specifico all'interno della matematica.

Calcolo

1. *Ambito del problema.*

'Calcolo' e anche 'conto' e 'computo': tre termini per uno stesso concetto o meglio tre termini per una famiglia di concetti abbastanza simili per essere raggruppati insieme, abbastanza diversi per non poter essere sussunti tutti sotto un unico schema. Una famiglia, un raggruppamento che nella costellazione delle voci portanti del progetto enciclopedico si situa tra meccanico e creativo, tra tecnica e filosofia, tra descrizione e spiegazione, tra pratica e teoria, tra concreto e astratto. Due citazioni. Per Lichtenberg, «il cosiddetto matematico pretende di essere ritenuto un profondo pensatore. Eppure tra di loro ci sono i piú grandi confusionari che esistano sulla faccia della terra, incapaci di qualsiasi cosa che richieda riflessione quando non si possa subito ridurre alla facile combinazione di segni che sono piú frutto del mestiere che del pensare» [1844-47, I, trad. it. p. 126]. Per Hobbes, «calcolare è cogliere la somma di piú cose... ragionare, dunque, è la stessa cosa che addizionare e sottrarre... non solo numeri ma anche un corpo a un corpo, ... un'azione a un'azione, un concetto a un concetto, un nome a un nome, e in questo consiste la filosofia» [*De corpore*, I, 1, § 2].

In molte lingue innegabilmente il termine richiama lo strumento fisico: il latino classico aveva *calculos ponere* 'porre sassolini', il latino medievale *calculare*, onde l'italiano *calcolo*, il francese *calcul* e l'inglese *calculus/calculation*. Tramontato l'abaco, 'calcolo' si associa spesso con 'macchina'. E *macchina calcolatrice* vuol dire molte cose: dalla calcolatrice meccanica al calcolatore elettronico programmabile «grande» o «piccolo» che sia: sono tutti riferimenti ormai familiari anche ai non-specialisti.

Ma la dipendenza dallo strumento è relativa. Tommaseo, nel *Dizionario dei sinonimi*: «CALCOLO e CALCULO. Computo o conto, cosí detto perché gli antichi da principio computarono per via di calcoli, o pietruzze. Ora ha un senso piú esteso, e significa ogni operazione, nella quale si tien computo o ragione non pur di numeri, ma eziandio di quantità o grandezze, quali che sieno. E si dice talvolta anche *Calcolo* o *Calculo*, o *Scienza del Calcolo*, quella parte delle matematiche la quale insegna a fare il calcolo. E dicesi Calcolo tanto l'Operazione del calcolare, quanto il Computo già finito».

Il rimando piú ovvio è a 'matematica', ma i due termini coprono due aree distinte e la sovrapposizione è solo parziale. C'è un calcolo non-matematico (per Jeremy Bentham c'è addirittura un calcolo del piacere e del dolore) e c'è una matematica non-calcolistica.

Ciò viene curiosamente riflesso dai dizionari. Un calcolo vi è definito come «ogni metodo che serve a eseguire operazioni matematiche» e un aggettivo ('aritmetico', 'algebrico', 'infinitesimale', ecc.) specifica la natura di tali operazioni. Ma si affianca all'accezione «rigorosa» il senso figurato: *previsione*,

congettura. Chi è piú attento allo «stile corretto» informa che «*calcolare*, o *far calcolo* nel significato *confidare*, *fare assegnamento*, *far conto*, *giudicare*, *stimare*, *considerare*, *valutare*, *ponderare*, *pensare e sim.* è modo che dispiace ai puristi» (Gabrielli, *Dizionario dello stile corretto*), pur concedendo che «l'uso antico e moderno dei due termini, anche da parte di buoni e ottimi scrittori, li rende tollerabili». C'è qualche attenuante per scrittori «buoni» e meno buoni: non si dà infatti né predizione scientifica né pianificazione razionale senza calcolo.

Di qui la vaghezza o meglio l'ambiguità ma anche la ricchezza del termine: spettro amplissimo di accezioni che vanno dall'aritmetica di un primitivo che non conta oltre cinque, a quella impostata sugli ultrarapidi calcolatori elettronici. Ma *calcolo non è sinonimo di manipolazione di numeri*. La «famiglia» si è arricchita di sempre nuovi componenti via via che è cresciuta l'importanza del calcolo, o meglio dei calcoli, nell'impresa scientifica e tecnologica ed è tramontata l'immagine della matematica come «scienza dei numeri e delle figure» per lasciare il posto a una complessa attività intellettuale difficilmente riducibile a una formula. Si può *calcolare*, dunque, con tante cose che non sono numeri: è calcolo, in senso lato, «l'operare con la logica, il tradurre lingue, il progettare circuiti, il giocare, il coordinare dispositivi di senso e di manipolazione e, in generale, assumere complicate funzioni associate al cervello umano» [Shannon 1953, trad. it. p. 94].

Benché nella storia del 'calcolo' o dei 'calcoli' il calcolo coi numeri a noi piú familiari (l'insieme dei numeri naturali 0, 1, 2, 3, 4, ... che indicheremo con **N**, e poi quello degli interi, quello dei razionali, quello dei reali e infine quello dei complessi, che indicheremo rispettivamente con **Z**, **Q**, **R**, **C**) sia stato un autorevole paradigma, il calcolo con entità diverse dai numeri ha acquistato sempre piú una sua consistenza e specificità (anche se, sotto un certo profilo, opportune *codificazioni* possono ricondurre calcoli non-numerici a calcoli numerici). Una dinamica presente in quello che il matematico italiano Giuseppe Peano chiama pressoché agli inizi del Novecento «il sogno» di Leibniz [Peano 1898]. Del resto, per Leibniz [citato in Bocheński 1956, trad. it. p. 357] «[necessita] una *caratteristica* della *ragione*, mediante la quale le verità, in qualsiasi dominio, si presenterebbero alla ragione in virtú di un metodo di calcolo come nell'aritmetica e nell'algebra». «Di conseguenza, quando sorgeranno controversie fra due filosofi, non sarà piú necessaria una discussione, come [non lo è] fra due calcolatori. Sarà sufficiente, infatti, che essi prendano in mano le penne, si siedano di fronte agli abachi e... si dicano l'un l'altro: *Calculemus!*» [Leibniz, citato *ibid.*]. La combinatoria di Leibniz adombra due accezioni chiave del calcolo: la manipolazione di un insieme finito di simboli secondo regole prefissate e la procedura effettiva.

Non daremo qui né una trattazione sistematica dei vari tipi di calcolo né una storia del calcolo: ci orienteremo invece nel labirinto degli indispensabili riferimenti di carattere specialistico alle tecniche del calcolo (e anche, dove lo riterremo opportuno, alla loro storia) usando come «filo di Arianna», per riprendere una metafora dello stesso Leibniz, una dicotomia fondamentale: «La matematica è una disciplina che può essere sviluppata, partendo dai suoi

aspetti piú familiari, in due opposte direzioni. La direzione piú comune è costruttiva e procede verso una complessità gradualmente crescente... L'altra direzione, che è meno comune, procede per analisi verso una sempre maggior astrazione e semplicità logica» [Russell 1919, trad. it. p. 11]. Ma l'opposizione non è rigida, i due termini interagiscono. Per questo, limitandoci entro l'orizzonte della matematica, abbiamo delineato non solo alcuni aspetti della transizione dal calcolo coi numeri al calcolo come «sistema formale» (§ 2), il ruolo centrale dell'analisi reale e complessa, *the Calculus* per eccellenza, come dicono ancor oggi gli Anglosassoni (§ 3), le caratteristiche specifiche della moderna analisi numerica (§ 4), ma abbiamo anche dedicato un certo spazio alla analisi della nozione di effettivo e allo studio della crescente complessità che l'approccio costruttivo sembra comportare. Piú precisamente, si è fatto cenno all'esplicazione della nozione di funzione «calcolabile» (o «computabile») (§ 5) e alla cosiddetta complessità computazionale (§ 6). Il riferimento ad algoritmi ideali (per esempio macchine di Turing) o reali (come gli esempi del § 6) non mira qui a una trattazione sistematica, ma solo ad approfondire la nostra concezione intuitiva di cosa sia un calcolo.

Tale approfondimento non necessariamente andrà in un'unica direzione. Già l'immagine intuitiva, come abbiamo premesso all'inizio del paragrafo, rivela una famiglia di concetti: a maggior ragione il passaggio a nozioni rigorosamente determinate aprirà nuove ramificazioni, destinate spesso a disorientare il lettore non matematico. Cosí del resto è avvenuto ogniqualvolta nuove idee hanno spento una tradizione di ricerca, mostrando che le procedure che la costituivano erano superate e hanno stabilito un nuovo paradigma: la continuità nello sviluppo delle teorie e il recupero del passato sono conquiste del dopo, di quando si è ristabilito l'equilibrio tra innovazione e tradizione.

Né c'è da stupirsi che sia cosí. La stessa teorizzazione scientifica sarebbe inutile se le rappresentazioni intuitive risultassero sempre adeguate ai bisogni che motivano la ricerca; inoltre la dicotomia intuizione/rigore è mobile. Muta nel tempo e talvolta anche bruscamente.

«Iniziare uno studente al calcolo è un po' come doveva essere il navigare nello stretto di Messina una volta: da un lato Cariddi che trascina l'imbarcazione nel gorgo, dall'altro Scilla che attende che la nave si infranga sulle rocce. Il gorgo che inghiotte tanti insegnanti è costituito da tutti quegli enunciati falsi circa quantità infinitamente piccole; le rocce su cui il principiante fa naufragio sono i solidi fondamenti dell'analisi. Un insegnamento adeguato del calcolo deve accuratamente eliminare tutti gli asserti privi di senso, ma allo stesso tempo fare a meno di ragionamenti pedantemente rigorosi. Se aggiungiamo che anche una semplice introduzione dovrebbe mirare a far capire allo studente il senso del calcolo piuttosto che a dargli un'abilità puramente meccanica nel maneggiare le formule, abbiamo piú o meno descritto le difficoltà che l'insegnante ha di fronte» [Menger 1945, p. 28].

Come la navigazione anche la mediazione tra questi due estremi – esposizione analitica ultraspecialistica e generico richiamo sintetico – richiede strumenti delicati. In questa sede le tematiche generali svolte negli articoli «Assioma/po-

stulato» e «Applicazioni» di questa stessa *Enciclopedia* costituiranno un termine di riferimento; in particolare saranno presupposti i primi elementi e le corrispondenti notazioni della teoria degli insiemi, delle strutture algebriche e topologiche che il lettore ritrova ampiamente spiegate e commentate in tali voci. Solo qualche paragrafo, data la complessità degli argomenti trattati, richiederà ulteriori riferimenti matematici (è il caso, per esempio, dei §§ 3.7 e 3.8).

2. *Dal calcolo coi numeri al calcolo logico.*

2.1. Preliminari sulla notazione.

Se certe comunità «primitive» riescono a far fronte alle esigenze pratiche disponendo nel loro linguaggio di nomi solo per i primi cinque o sei numeri, la padronanza del calcolo con numeri grandi appare oggi una necessità della società civile. Questa considerazione che sembra ovvia è il punto di arrivo di una vicenda che ha visto per lunghi periodi la scissione tra rigore geometrico e abilità aritmetica e algebrica, tra astrazione e pratica del calcolo, tra tecnica calcolistica e numerazione scritta.

È noto che nelle antiche scritture (babilonese esclusa) il valore di un numero si otteneva come somma dei valori convenzionalmente attribuiti ai segni elementari che costituivano il simbolo che li denotava, cioè quel che i Latini chiamavano *nota*. Nella scrittura dei Romani, per esempio, 36 viene denotato da XXXVI, una *nota* ove compaiono tre segni X che stanno ciascuno per dieci, un segno V che sta per cinque e un segno I che sta per uno: $10+10+10+5+1=36$. Si comprende subito come tale scrittura fosse particolarmente inadatta a un calcolo semplice e sistematico.

L'abaco, di tradizione antichissima, costituí una premessa per l'introduzione dei segni numerici «arabi», in quanto in esso il concetto di numerazione posizionale era inconsciamente anticipato. Ma che dall'invenzione del calcolo con l'abaco non sia derivata immediatamente la notazione posizionale non deve stupire: come l'elaborazione intellettuale in certe culture orali non sembra necessitare della parola scritta, cosí per lungo tempo scrittura del numero e calcolo sono rimasti atti distinti e indipendenti.

Il nostro attuale sistema di conto è pervenuto in Europa, da fonti arabe, in scritti isolati nel XII secolo: nel *Liber Abaci*, con cui in Italia viene diffusa nel 1202 la conoscenza delle «novem figurae yndorum» e del segno 0 «quod arabice zephirum appellatur», Leonardo Pisano già appare pienamente consapevole del fatto che con la nuova notazione il procedimento di calcolo viene ridotto a un certo numero di calcoli elementari su numeri inferiori a 10.

Nel sistema decimale si scompone infatti ogni numero naturale secondo le potenze del numero 10: 36 è $3\times10^1+6\times10^0$; 5681 è $5\times10^3+6\times10^2+8\times10^1+1\times10^0$; ecc. In linea di principio non c'è ragione di non considerare la scomposizione dei numeri naturali secondo le potenze di un *qualsiasi* numero prefissato $n>1$. Cosí facendo si ottengono enunciati generali i cui casi speciali per $n=10$ sono ben noti.

È immediata la procedura di calcolo che permette di trovare la rappresentazione n-aria di un dato naturale a. Si determina innanzitutto il numero $t>0$ che soddisfa le diseguaglianze $n^{t+1}>a\geq n^t$; dopo di che si ha via via:

$$\begin{array}{lll} a=q_tn^t+r_t & \text{con } 0\leq r_t<n^t & 0<q_t<n \\ r_t=q_{t-1}n^{t-1}+r_{t-1} & \text{con } 0\leq r_{t-1}<n^{t-1} & 0\leq q_{t-1}<n \\ \vdots & \vdots & \vdots \\ r_2=q_1n+r_1 & \text{con } 0\leq r_1<n & 0\leq q_1<n. \end{array}$$

Si può allora esprimere a (in *un unico* modo) come $q_tn^t+q_{t-1}n^{t-1}+\ldots+q_1n+q_0$ ove si è posto $r_1=q_0$; cioè possiamo associare ad a la sua rappresentazione n-aria $(q_tq_{t-1}\ldots q_1q_0)_n$: $q_0, q_1, \ldots, q_t$ si dicono *cifre* di a in *base* n.

Varie ragioni – per esempio esigenze proprie della tecnologia dei calcolatori, ma non solo – possono consigliare rappresentazioni con $n\neq10$, per esempio $n=2$, $n=12$, $n=16$, ecc. Per $n=16$, poniamo, abbiamo bisogno delle sedici cifre 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F: il numero 48 543, per esempio, in base sedici si scrive BD9F, ecc. Dalla rappresentazione esplicita

$$a=q_tn^t+\ldots+q_0$$
$$b=q'_sn^s+\ldots+q'_0$$

si ricava immediatamente che in ogni sistema n-ario si possono eseguire le operazioni di addizione $a+b$, di moltiplicazione $a\times b$, ecc. in modo analogo a come le si esegue in base dieci. Cosí, per esempio, si dominano addizione e moltiplicazione non appena si siano apprese le rispettive «tabelline» del sistema n-ario. Per esemplificare riportiamo la tabella di moltiplicazione in base sedici:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	10	12	14	16	18	1A	1C	1E
3	0	3	6	9	C	F	12	15	18	1B	1E	21	24	27	2A	2D
4	0	4	8	C	10	14	18	1C	20	24	28	2C	30	34	38	3C
5	0	5	A	F	14	19	1E	23	28	2D	32	37	3C	41	46	4B
6	0	6	C	12	18	1E	24	2A	30	36	3C	42	48	4E	54	5A
7	0	7	E	15	1C	23	2A	31	38	3F	46	4D	54	5B	62	69
8	0	8	10	18	20	28	30	38	40	48	50	58	60	68	70	78
9	0	9	12	1B	24	2D	36	3F	48	51	5A	63	6C	75	7E	87
A	0	A	14	1E	28	32	3C	46	50	5A	64	6E	78	82	8C	96
B	0	B	16	21	2C	37	42	4D	58	63	6E	79	84	8F	9A	A5
C	0	C	18	24	30	3C	48	54	60	6C	78	84	90	9C	A8	B4
D	0	D	1A	27	34	41	4E	5B	68	75	82	8F	9C	A9	B6	C3
E	0	E	1C	2A	38	46	54	62	70	7E	8C	9A	A8	B6	C4	D2
F	0	F	1E	2D	3C	4B	5A	69	78	87	96	A5	B4	C3	D2	E1

Le tabelle diventano ovviamente tanto piú semplici quanto piú piccolo è il numero n. Per $n=2$ abbiamo rispettivamente:

Addizione aritmetica

+	0	1
0	0	1
1	1	10

Moltiplicazione aritmetica

×	0	1
0	0	0
1	0	1

Peraltro si ha l'inconveniente che per n piccolo un elevato numero di cifre è necessario per rappresentare numeri anche non molto grandi. Cosí il numero 402 in base dieci si scrive 110010010 in base due.

Sul sistema binario torneremo piú oltre (cfr. §§ 2.4 e 2.6); concludiamo osservando che si dànno procedure standard con cui è agevole passare da una base n a un'altra base m e rinviando a Knuth [1969, pp. 162-76] per ulteriore informazione, in particolare sull'impiego di basi negative, ecc. Nel seguito, salvo avviso contrario, impiegheremo il tradizionale sistema decimale, il che appunto non riduce la generalità del nostro discorso.

2.2. Le quattro operazioni elementari e i numeri naturali.

Non è casuale che la parola 'algoritmo' nella tradizione matematica dell'Occidente abbia avuto dapprima il significato di «calcolo mediante decimali» (cioè, cfr. § 2.1, di calcolo «posizionale»). Ancora Nicolò Tartaglia spiega all'inizio del libro secondo del suo *General Trattato di numeri et misure* che «la Pratica Arithmetica, come afferma Giovan de Sacrobusto, fu data Compendiosa in luce da un Philosopho detto Algo et per questa causa fu chiamata Algorismo, over Algorithmo» [1556, p. 3]. Il «Philosopho Algo» è al-Khuwārizmī, già nella prima traduzione latina della sua *Aritmetica* battezzato Algoritmo (il titolo del libro era infatti *Algorithmi de numero Indorum*); Giovan de Sacrobusto è Giovanni di Sacrobosco (versione latina del nome John Holywood), astronomo e matematico inglese del XIII secolo.

La «pratica aritmetica» di cui parla Tartaglia sarà destinata a fornire per secoli il paradigma di quel che deve essere «un calcolo»: essa consta in primo luogo di quegli «atti» che oggi costituiscono le quattro operazioni elementari: «iongere», «cavare», «moltiplicare» e «partire», per usare la terminologia di uno dei primi manuali di aritmetica a stampa, *Larte de labbacho*, pubblicato a Treviso nel 1478 a beneficio dei giovani veneti che intendevano darsi alla mercatura. Ciascun atto è ivi caratterizzato da un suo proprio «articulo»: «Iongere ha per suo articulo et. Cavare ha per suo articulo de. Moltiplicare ha per suo articulo fia. Partire ha per suo articulo in» [cit. in Picutti 1977, p. 66]. Tali

«articuli» a partire dal Cinquecento sono destinati a essere rimpiazzati dalle parole 'piú', 'meno', 'per', 'diviso' mentre si introducono i corrispondenti segni, $+ \; - \; \times \; :$. Ma il modo di esprimersi dell'ignoto autore quattrocentesco ci offre un filo rosso: come la grammatica regge l'uso degli articoli nel linguaggio quotidiano, cosí le parole 'piú', 'meno', ecc. vanno usate secondo una grammatica, che compendi le regole della «pratica aritmetica» proprio come la grammatica italiana compendia le regole della lingua italiana. Piú oltre daremo la grammatica del calcolo coi numeri naturali come grammatica di un «linguaggio perfetto» (cfr. § 2.7). Qui invece vediamo come le regole (associative, commutative, distributive, ecc.) autorizzano degli schemi operativi che nella stessa terminologia sono spie ora delle motivazioni pratiche ora delle giustificazioni teoriche.

Prendiamo in esame per esempio una sottrazione, $222-108$. Siamo soliti eseguirla in questo modo: $2-8$ non si può effettuare in quanto 8 è maggiore di 2; prendiamo «in prestito» una decina dal 2 (che diventa 1); $12-8$ fa 4, che scriviamo. Si è in tal modo sottratto il numero 8 della prima decina dal numero 12 della seconda decina. «Il procedimento *per prestito* era, secondo Tartaglia, quello piú antico. È ancora usato anche il procedimento *senza prestito*; dovendosi, ad esempio, sottrarre 39 da 62, si aumenta di dieci il 2 del minuendo (che diventa 12) e il 3 del sottraendo (che diventa 4). Eseguiamo poi $12-9=3$ e $6-4=2$ ottenendo il risultato 23». In un terzo procedimento in uso anticamente si venivano a sottrarre solo due numeri della prima decina. Dovendosi, per esempio, effettuare $52-29$ si procedeva cosí: $2-9$ non si può eseguire; 9 al 10 manca 1; $1+2=3$, che scriviamo; $4-2=2$, che scriviamo. «Non limitando la somma al caso in cui la cifra del sottraendo superi la corrispondente cifra del minuendo, l'operazione si trasforma di fatto in una *addizione tra il minuendo e il complemento del sottraendo*... intendendosi per *complemento* di un numero la sua differenza dalla potenza della base a esso immedia-

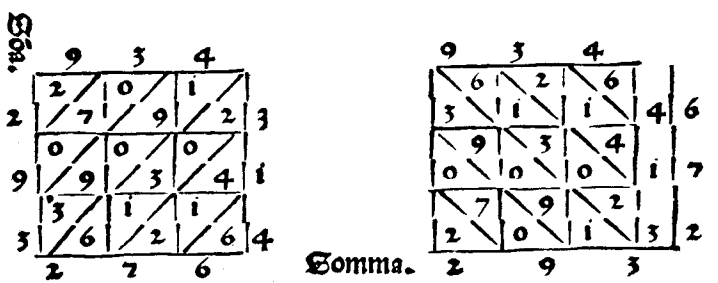


Figura 1.

Schema «a gelosia» da *Larte de labbacho*. Moltiplicando (per esempio 934) e moltiplicatore (per esempio 314) si scrivono ai lati di un rettangolo suddiviso in caselle. Si riempiono poi le caselle con i prodotti parziali, come nella tavola pitagorica. Si somma infine in diagonale (nell'esempio il risultato è 293 276). Si noti che col termine 'somma' si denota qui il prodotto.

tamente superiore» [Picutti 1977, p. 67, anche per altri interessanti dettagli].

Se la terminologia – «con prestito», «senza prestito» – rimanda immediatamente ai libri dei mercanti, lo schema adombra un ordine di idee che prelude ai numeri relativi – cosí «assurdi» per i matematici cultori del rigore ancora nel Seicento e nel Settecento, ma cosí «naturali» in certe situazioni (crediti/debiti, profitti/perdite).

Per fare un altro esempio, lo schema della moltiplicazione detto «a gelosia» (fig. 1), al di là del pittoresco nome («gelosia intendiamo quelle graticelle che si costumano mettere alle finestre de le case dove habitano done; acio che non si possino facilmente vedere», spiega Pacioli [cit. in Picutti 1977, p. 70]), fornisce una procedura che riduce al minimo la possibilità di sviste e permette, in poco spazio, di maneggiare numeri anche molto grandi.

La divisione è notoriamente l'operazione elementare piú delicata: a parte la *vexata quaestio* della divisione per 0, l'operazione inversa della moltiplicazione – dati a e b trovare x tale che $a=bx$ – ha significato solo se a è multiplo di b. Tuttavia, anche quando ciò *non* si verifica, è possibile determinare univocamente «senza uscire dal sistema dei numeri naturali» (vedremo nel § 2.3 cosa questa locuzione significa esattamente) due numeri q e r tali che $a=bq+r$ con $0 \leq r < q$, detti rispettivamente «quoziente» e «resto» (il «partitore» e l'«avanzo» nel medioevo). Ma la storia degli schemi via via utilizzati è per lo meno curiosa.

Uno dei piú adoperati fino a tutto il Seicento è infatti quello «per battello» o «per galera», denominazione che deriva dall'aspetto simile alla galera (cfr. fig. 2) che lo schema scritto assume a fine operazione. Troppo lungo sarebbe qui descriverne il funzionamento [si veda Picutti 1977, pp. 86-89]: basti dire

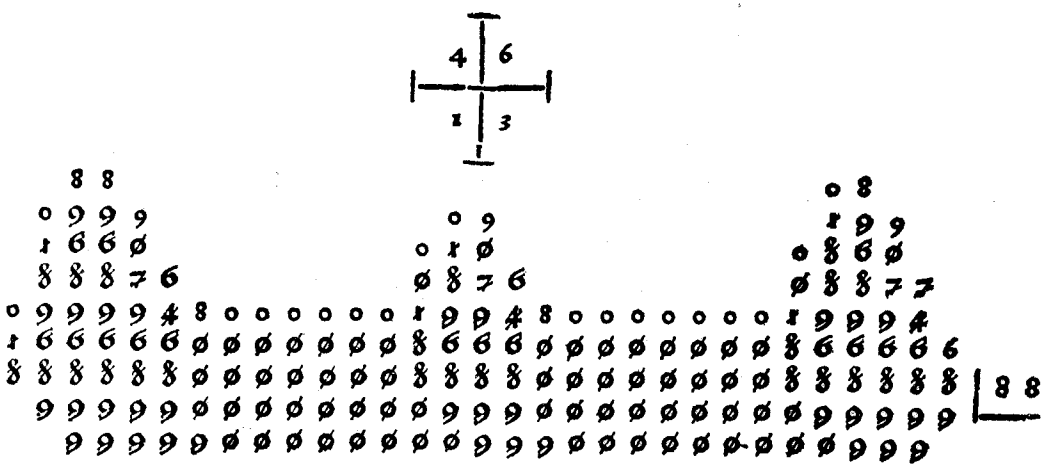


Figura 2.
Schema della divisione «per galera» [Tartaglia 1556, p. 31].

che agli occhi stessi di coloro che vi ricorrevano ogni volta che si imbattevano in una divisione di una certa difficoltà, il procedimento appariva cosí astruso da rappresentare una «sfida» al talento matematico: in tale ambito il calcolo appare dunque un pezzo di bravura per specialisti. Scrive per esempio Tartaglia: «Costumasi in Venetia, quando che un discepolo ha inteso ben questo partire per batelo, a darvi per ispasso alcuni partiri, che nella espeditione di quelli ne danno una figura simile a una galea materiale, con la prova et poppa ellevata anchora nel luogo dell'arboro et le depenature rapresentano poi li remi, onde per non preterire a tal ordine te ne voglio dare alcuni, quali ti faran tal effetto, delliquali il primo sarà questo partitore 888888000000088880000000088888, per questo numero 999990000000099900000000009999... il medesimo ti verrà a partire 77777770000000777700000000077777777 per 888880000000088800000000008888888 et cosí infiniti altri da te medesimo ne potrai trovare, che ti faranno un simil effetto» [1556, p. 35]. Nella figura 2 riportiamo lo schema relativo al primo esempio, il quoziente è 88, il resto 8896800000000968000000000008976.

È del matematico, non meno che del poeta, «il fin: la meraviglia»? Il calcolo sembra oscillare tra i due poli dell'opposizione procedimento meccanico/creativo ovvero svolgimento di una procedura in modo irriflesso/consapevole. Ma la 'struttura fine', per cosí dire, di tale opposizione rivela la presenza di insospettate mediazioni. Per avere risposta al quesito di come sia nato un procedimento del genere e soprattutto come possa essere rimasto *il* metodo generale per secoli si individua allora una connessione con le procedure di fatto impiegate sull'abaco, strumento di calcolo per eccellenza ancora ai tempi di Pascal e di Newton, in particolare con la tecnica detta «divisione aurea» di cui la divisione «per galera» risulta probabilmente la trasposizione scritta [cfr. Picutti 1977, pp. 88 e 106-10].

Possiamo qui solo accennare alla transizione dalla divisione per galera a quella detta «per danda» che è il tipo di divisione tuttora in uso. Un paradigma di tale transizione si trova alla fine del libro secondo del *General Trattato* di Tartaglia ove sono riportati alcuni schemi semplificati di divisione per galera (fig. 3). La «scoperta» di schemi piú «semplici», cioè piú maneggevoli e piú applicabili, è certo un frutto della «ingegniosità» del ricercatore: ma ingegnosità è sinonimo spesso di capacità di astrazione *dagli* schemi che regolano «secondo l'ordinario» la pratica del calcolo.

Concludiamo queste brevi note sulle quattro operazioni nel sistema dei numeri naturali (zero *incluso*) osservando che nel calcolo della somma e del prodotto di due numeri naturali qualsiasi, nel calcolo della differenza di due numeri di cui il secondo non sia maggiore del primo, e infine nella determinazione del quoziente e del resto della divisione di due numeri (cfr. sopra, p. 385) gli unici errori possibili sono gli sbagli soggettivi di chi impiega le varie procedure. Di qui la richiesta di maggior semplicità che sottende l'impiego di non pochi degli schemi per le quattro operazioni; di qui anche «gli artifizi» che permettono di «vedere» certi risultati saltando alcuni passaggi dello schema. Nella divisione 438 811 : 9, per esempio, possiamo vedere che il resto è 7 «infilzando le figure» come diceva Luca Pacioli, cioè addizionando le cifre di 438 811 e ottenendo

Figura 3.

Tre schemi per dividere 888 880 per 9999 offerti da Tartaglia. Il primo è quello «secondo l'ordinario» e cioè per galera. Il secondo ne differisce nella parte superiore in conseguenza della «partitione fatta a principiare, a multiplicare, e a sottrar dalla banda destra». L'ultimo schema, a parte la posizione del divisore 9999 e del quoziente 8, è lo schema a danda, quello che rappresenta per noi «l'ordinario».

25 e quindi addizionando le cifre di 25, che dà 7. È lo stesso ordine di idee che sottende tecniche come la celebre «prova del 9». Si tratta di un tipico esempio di questioni di divisibilità che troveranno il loro quadro naturale nella teoria gaussiana delle congruenze, ove una notazione ordinata e compatta permette di ritrovare tutte le giustificazioni piú o meno ad hoc che di tali «artifizi» avevano fornito i matematici precedenti. Un salto di qualità che bene illustra come il passaggio a un maggior livello di astrazione permetta di cogliere piú profondamente il senso di tutta una serie di pratiche impiegate in concreto. Vi faremo un riferimento piú dettagliato nel § 2.4.

2.3. Dal calcolo coi naturali a quello con gli interi relativi e coi razionali.

Non adoperiamo però nel «far di conto» solo i numeri naturali, ma anche i numeri relativi o, come si diceva una volta, i numeri «con segno», i numeri razionali (press'a poco quelle che si chiamano comunemente frazioni) e infine i numeri reali e i numeri complessi. «Fra di essi, i numeri *naturali* sembrano essere i "numeri" per eccellenza, i veri e propri numeri, con un'assoluta priorità su tutti gli altri; tanto che Kronecker una volta ebbe a scrivere press'a poco una frase come questa: "I numeri naturali li ha fatti Dio, tutti gli altri li hanno fabbricati gli uomini". A parte questa incontrollabile ipotesi sul loro fabbricatore, la priorità dei numeri naturali posa in primo luogo su una molto probabile verità storica, e in secondo luogo sul fatto che mediante piú o meno complicati accorgimenti tecnici il calcolo sugli altri numeri può venir ridotto a una serie di operazioni sui numeri naturali» [Preti 1953, p. 170].

Utilizziamo questo accenno come traccia. Oltre ad aggettivi come 'uno', 'due', 'tre', ... anche le lingue piú primitive hanno termini numerici quali 'un mezzo', 'un terzo', 'un quarto'; dire invece che segni quali -1 o a maggior ragione $\sqrt{2}$, $\sqrt{-1}$ stanno per numeri è uso di questi ultimi secoli (cfr. oltre, §§ 3.2, 3.3 e 3.6). Ma questo sviluppo è proprio connesso con la pratica del calcolo. Supponiamo che la considerazione di un problema, magari un banale problema della vita di tutti i giorni, ci abbia portato a formulare l'equazione $x+3=2$ (pensiamo a un mercante dei tempi andati che vuol sapere quanto denaro aveva «al banco» prima di portare il proprio conto a 2 fiorini versandone 3). L'equazione non si risolve in termini di numeri naturali, ma se ammettiamo che si parli di numeri negativi possiamo allora scrivere $x=-1$ (il mercante aveva col banco il debito di 1 fiorino). Possiamo rappresentare tali numeri ponendo su una retta segni a intervalli uguali a sinistra di un punto che convenzionalmente scegliamo per rappresentare lo 0 (fig. 4).

In un analogo ordine di idee dobbiamo ammettere numeri come $3/2$ per parlare di soluzione esatta di equazioni come $2x-3=0$. Con essi si ha una notevole aggiunta ai numeri che possono venir rappresentati dai punti di una retta. Infatti, *tra* due frazioni qualsiasi, possiamo sempre trovarne un'altra, il che è come dire che vi è un'infinità di frazioni in qualsiasi intervallo finito come [0, 1]. Tuttavia non dobbiamo presumere di aver individuato con questo ampliamento tutti i punti della retta. A suo tempo l'immagine della scienza dei pitagorici venne messa in crisi dalla «scoperta» del fatto che, se costruiamo un

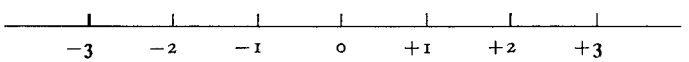


Figura 4.

La rappresentazione sulla retta degli interi relativi fornisce una suggestiva immagine geometrica. A sinistra del punto che rappresenta lo 0 sono collocati gli interi negativi; a destra gli interi positivi.

quadrato il cui lato ha lunghezza di un'unità e se, a partire dall'origine del lato, tracciamo la diagonale del quadrato, il punto che individuiamo sulla retta non è uno di quelli cui (fig. 5) finora abbiamo assegnato numeri (cfr. oltre, § 3.2). Ma queste lacune e infinite altre vengono colmate con un terzo ampliamento del concetto di numero, che viene a comprendere gli irrazionali algebrici, come $\sqrt{2}$ e gli irrazionali trascendenti come π. Con i primi possiamo parlare di risoluzione di certe equazioni algebriche, come $x^2-2=0$; con gli altri possiamo completare il continuo lineare. Infine, con un quarto ampliamento riconosciamo nel numero «immaginario» $\sqrt{-1}$ una radice propria dell'equazione $x^2+1=0$. Qui l'intuizione geometrica sembra venir meno: sulla retta non vi è un punto che corrisponda a $\sqrt{-1}$. Va da sé che l'introduzione di «nuovi» numeri (relativi, razionali, reali, complessi) può avere delle conseguenze controintuitive, almeno a prima vista. Certi modi linguistici non sono trasferibili dagli usuali numeri naturali, poniamo, ai complessi: non ha senso, per esempio, dire che in una stanza ci sono $15+3\sqrt{-1}$ uomini, ecc.

Ma allora cosa sono i numeri? Un quesito cui si può rispondere in vari modi. Nel § 3 illustreremo alcuni aspetti del calcolo differenziale e integrale nei quali sono utilizzati come strumento principe i numeri reali e i numeri complessi. Nel seguito di questo paragrafo vedremo invece come l'impulso all'ampliamento (a partire dai naturali), basato sulla possibilità di calcolare con simboli utilizzando opportune regole formali, sia collegato allo sviluppo dell'algebra: questa è appunto «la funzione creativa della forma», per usare una fortunata locuzione degli algebristi dell'Ottocento.

«Dubito... che sia pratico trattare radici, potenze, serie, logaritmi, ecc., sia pur elementarmente, *soltanto* con numeri (senza tutti gli altri sussidi algebrici, e *in fact* senza presupposti di nozioni di algebra elementare). Per quanto buono sia l'impiego di esempi numerici per le spiegazioni, tuttavia qui la limitazione a numeri mi riesce meno evidente che la semplice trattazione algebrica con $a+b$, appunto perché l'espressione generale algebrica è piú semplice ed evidente» (Engels, lettera a Marx, Manchester, 30 maggio 1864).

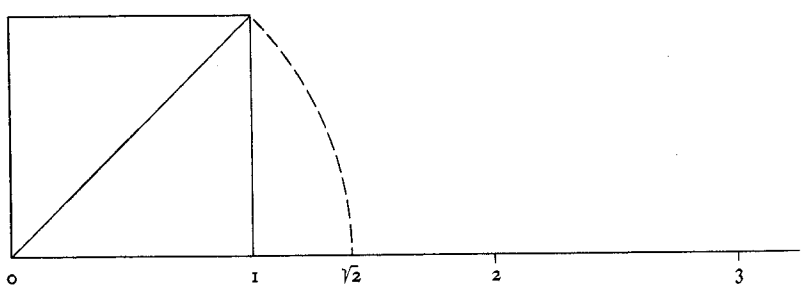


Figura 5.
Costruzione sulla retta dell'immagine di $\sqrt{2}$.

Per quanto riguarda la rilevanza di un approccio di tipo algebrico ai numeri complessi rimandiamo il lettore al § 3.6. Qui osserviamo che l'insistenza sull'aspetto algebrico è motivata da questo semplice fatto: le nozioni di addizione e di moltiplicazione appropriate nel calcolo coi naturali non possono applicarsi immediatamente in un calcolo di numeri di altro tipo. Lo studente delle medie inferiori associa spesso all'apprendimento delle regole dei segni per la moltiplicazione degli interi relativi

$$(+a)(+b)=+ab$$
$$(+a)(-b)=-ab$$
$$(-a)(-b)=+ab$$

l'impressione che si tratti di ricette che vanno apprese a memoria perché, poniamo, 'meno' per 'meno' *deve* fare 'piú'. Ma la parola 'deve' è mal scelta: in realtà non si tratta di necessità, ma di convenzione: come scriveva Gauss a Bessel nel 1811 e come ribadiva poi Hankel, tali regole «sono stipulazioni arbitrarie, scelte allo scopo di conservare il formalismo nel calcolo» [cit. in Waismann 1936, trad. it. p. 53]. Le regole basilari del calcolo coi numeri sono motivate in concreto dalle piú svariate pratiche, ma finiscono coll'indicare in astratto certe condizioni logiche che devono essere soddisfatte dalle operazioni di qualsiasi calcolo che vogliamo ancora considerare un «calcolo coi numeri».

Quelle che prima abbiamo chiamato «regole di calcolo» si mutano allora in «proprietà formali». Un simile slittamento di prospettiva bene si individua in quello che Peacock battezzò nel 1833 «the principle of the permanence of equivalent forms» e che divenne noto in seguito come «principio di permanenza delle proprietà formali». Tale principio euristico sul piano della teoria giustifica il passaggio ai nuovi sistemi di enti impiegati nella pratica, purché in tali sistemi siano mantenute «le regole generali dell'algebra». Anche un punto di vista conservatore può sottenderne l'utilizzazione: è il caso di tutti quei matematici che consideravano ogni innovazione un passo obbligato cui erano costretti per risolvere i problemi posti nello stadio precedente, «senza concepire l'algebra astraendo dalle sue esemplificazioni e senza tentare di inventare nuovi calcoli per portare lo sviluppo il piú avanti possibile» [Kneale 1962, trad. it. p. 453].

È con l'emergere della concezione astratta dell'algebra tipica dell'Ottocento che la situazione si è sbloccata. Peacock non fu infatti il solo; Gregory nel 1838 pubblica l'articolo *On the Real Nature of Symbolic Algebra*; tra il 1839 e il 1844 compaiono i quattro saggi *On the Foundations of Algebra* di De Morgan; contemporaneamente emergono calcoli decisamente nuovi rispetto alla pratica matematica corrente: del 1844 sono la fondamentale *Ausdehnungslehre* di Grassmann, che attua il progetto leibniziano di un calcolo geometrico (ponendo le basi del calcolo delle forme differenziali esterne in senso moderno) e il primo saggio sui quaternioni di Hamilton. Questi richiami paiono sufficienti; va aggiunto però che solo una visione deliberatamente astorica può presentare esiti del genere come generalizzazioni fini a se stesse: il progetto hamiltoniano, per esem-

pio, trovava la sua motivazione nell'esigenza di un calcolo che, per il moto nello spazio tridimensionale, facesse ciò che la teoria dei numeri complessi sembrava fare adeguatamente per il moto in un piano. Come i numeri complessi sono esprimibili nella forma $x+yi$ (cfr. § 3.6) cosí i quaternioni di Hamilton sono esprimibili nella forma $x+yi+zj+wk$ (ove le lettere i, j, k rappresentano rotazioni in tre piani perpendicolari l'uno all'altro). Ma a differenza del sistema dei complessi, quello dei quaternioni non soddisfa tutte le usuali «leggi dell'algebra»; com'è noto, proprio per conservare altre regole, Hamilton dovette abbandonare la regola commutativa della moltiplicazione (nell'algebra dei quaternioni è, per esempio, $ij=-ji$). Un fenomeno per certi versi analogo si ripresenta in un altro sistema ipercomplesso, di poco posteriore (1845 e 1847) a quello hamiltoniano, quello degli ottetti di Cayley ottenuti come coppie ordinate di quaternioni; qui, oltre alla proprietà commutativa, viene abbandonata anche quella associativa per la moltiplicazione.

Un esame approfondito dei sistemi numerici – dagli interi relativi ai complessi – mostra che anche in tali casi il passaggio da uno stadio a uno stadio successivo esige l'abbandono di *qualche* legge: per esempio, come il lettore può agevolmente verificare, il passaggio dal sistema dei naturali a quello degli interi relativi impone la rinunzia alla legge di monotonia della moltiplicazione: cfr. su questo punto le penetranti osservazioni di Waismann [1936, trad. it. pp. 58-63]. Se ancora pensiamo che con tali leggi si «colga» la «natura» dei numeri come enti a sé, per «numeri» dobbiamo allora intendere *soltanto* i numeri naturali e gli enti degli altri sistemi sono «numeri» solo in senso pickwickiano. Ma una volta riconosciuto che il punto di vista *essenzialistico* non è necessario per «potenziare» il calcolo, l'attenzione viene diretta alle formule che forniscono definizioni implicite dei vari tipi di espressioni numeriche: a seconda che si voglia privilegiare l'aspetto calcolistico o quello formale tali formule verranno viste come regole speciali di calcolo o rispettivamente come assiomi da cui derivare teoremi. L'importante sarà comunque l'enunciazione non ambigua di tali formule. Sulla opposizione essenzialismo/nominalismo ritorneremo nel § 2.7.

Ci sono dunque vari tipi di numeri e corrispondentemente vari tipi di calcolo (nell'accezione tipicamente algebrica di manipolazione formale di simboli).

Il passaggio dai naturali agli interi relativi e dagli interi relativi ai razionali (e per ora fermiamoci qui) non è però un semplice processo di generalizzazione: se dico, per esempio, che ho invitato tre ospiti, posso sostituire al 'tre' della lingua comune il '3' dei naturali, ma non il '+3' degli interi relativi: altrimenti avrebbe senso anche parlare di un invito di '−3' ospiti. A rigore il sistema dei naturali e quello degli interi sono due sistemi di numeri distinti (e lo stesso si può dire negli altri casi): $2-3$ resta un problema irrisolubile nel sistema dei naturali, quel che si risolve con l'introduzione del sistema degli interi è il problema «corrispondente» $(+2)-(+3)$. L'uso di questa locuzione implica che si può isolare nel sistema dei relativi un opportuno sottosistema (costituito nel caso da zero e dai numeri positivi) che viene agevolmente «identificato» con i

numeri naturali: la nostra esposizione è volutamente informale, ma, ovviamente, queste stesse considerazioni sono suscettibili di una trattazione rigorosa (cfr. anche § 3.1).

2.4. Concetto di corpo. Corpi finiti. Corpi ordinati.

Fermiamoci ancora sul sistema dei numeri razionali (per cui possiamo svolgere un discorso analogo a quello con cui abbiamo concluso il § 2.2; cfr. anche § 3.1). Com'è noto, tale sistema costituisce un cospicuo esempio di corpo commutativo (o campo): per corpo (commutativo) intendiamo un sistema **A** costituito da un insieme A, da due applicazioni binarie a un sol valore $+$ e $\times$ di $A\times A$ in A, da due elementi specifici distinti 0 e 1, da un'applicazione a un sol valore $-$ di A in A e di una applicazione a un sol valore $^{-1}$ di A^* in A (ove A^* denota l'insieme degli elementi di A diversi da 0) in modo che valgono gli assiomi seguenti:

I.1.	*a*)	Per ogni a, b in A,	$a+b=a+b$	proprietà commutative
	b)	Per ogni a, b in A,	$a\times b=b\times a$	
I.2.	*a*)	Per ogni a, b, c in A,	$(a+b)+c=a+(b+c)$	proprietà associative
	b)	Per ogni a, b, c in A,	$(a\times b)\times c=a\times(b\times c)$	
I.3.		Per ogni a, b, c in A,	$a\times(b+c)=(a\times b)+(a\times c)$	proprietà distributiva
I.4.	*a*)	Per ogni a in A,	$0+a=a$	
	b)	Per ogni a in A,	$1\times a=a$	
I.5.		Per ogni a in A,	$a+(-a)=0$	
I.6.		Per ogni a in A^*,	$a\times a^{-1}=1$.	

Gli assiomi **I** ricostruiscono adeguatamente il complesso di regole su cui si fonda la pratica del calcolo letterale con le quattro operazioni elementari, ove, come si dice usualmente nei manuali, le lettere a, b, c, ... «stanno per» delle «quantità» (di solito numeri razionali): in particolare le applicazioni $-$ e $^{-1}$ permettono di trattare le inverse dell'addizione $+$ e della moltiplicazione $\times$: $a-b$ abbrevia $a+(-b)$ e $a:b$ (o a/b) abbrevia $a\times b^{-1}$: la restrizione ad A^* in I.6 corrisponde al «divieto» di dividere per 0, ecc.

Gli assiomi della teoria astratta dei corpi valgono pure in sistemi molto diversi dal sistema dei razionali. Per rendercene conto basterà un breve accenno alla teoria delle congruenze, la cui prima trattazione sistematica si trova nelle *Disquisitiones arithmeticae* [1801] di Gauss. Due interi relativi r e s si dicono congrui modulo m (m relativo ovviamente diverso da 0 e da 1) – si scrive seguendo la notazione gaussiana $r\equiv s$ mod m oppure $r\equiv s$ se non c'è pericolo di confusione – se e solo se la differenza $r-s$ è divisibile per m, cioè se divisi per m i numeri r e s dànno lo stesso resto. Si mostra agevolmente che la relazione di congruenza mod m è una relazione riflessiva ($r\equiv r$), simmetrica (se $r\equiv s$, allora $s\equiv r$) e transitiva (se $r\equiv s$ e $s\equiv t$, allora $r\equiv t$). Tali proprietà motivano tra l'altro la scelta del simbolo $\equiv$. «Abbiamo adottato questo segno a

causa dell'analogia tra uguaglianza e congruenza», precisa Gauss in una nota in calce dell'articolo 2 delle *Disquisitiones*; ma, riferendosi all'*Essai d'une théorie des nombres* (1797) di Legendre aggiunge subito che se «per la stessa ragione [questi] ha usato lo stesso segno per uguaglianza e congruenza» occorre fare una distinzione «per evitare ambiguità».

Limitiamoci ora a m intero positivo (ciò non è restrittivo, in quanto la congruenza mod $-m$ è identica alla congruenza mod m) e ripartiamo gli interi relativi in classi avendo cura che tutti i membri di ciascuna classe siano tra loro congruenti. Il numero di classi distinte (classi di congruenza o di resto) che otteniamo è proprio m e ciascuna di queste classi può venir rappresentata da uno degli m numeri non negativi inferiori a m (appunto i resti della divisione per m: cfr. fig. 6); inoltre possiamo anche definire una addizione e una moltiplicazione per classi di resto mod m ponendo:

$$[r]+[s]=[r+s]$$
$$[r]\times[t]=[r\times t].$$

Si tratta di definizioni «ben poste» in quanto le operazioni in definitiva risultano due applicazioni a un sol valore, cioè la somma $[r+s]$ e il prodotto $[r\times s]$ sono ancora due classi mod m e vengono univocamente determinate dai rappre-

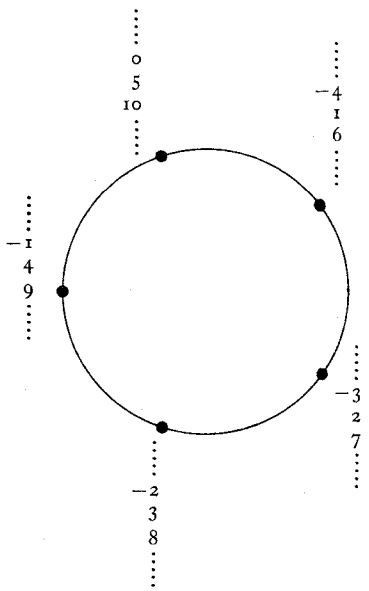


Figura 6.

Rappresentazione geometrica degli interi relativi modulo 5. Il lettore confronti con la rappresentazione degli interi relativi nella figura 4.

sentanti $r+s$ e $r\times t$ rispettivamente: per rendersene conto basta vedere questo calcolo dei resti come un calcolo coi relativi ove la somma di due numeri r, s non è piú l'usuale somma, ma la somma mod m, cioè il resto della divisione di $r+s$ per m, e analogamente il prodotto di r per s non è piú l'usuale prodotto, ma il prodotto mod m, cioè il resto della divisione di $r\times s$ per m. Se poi m è un numero primo (cioè se gli unici interi positivi che dividono m sono 1 e m stesso), il sistema delle classi mod m rispetto a tali operazioni costituisce un corpo, assumendo come 0 e 1 del corpo le classi [0] e [1] rispettivamente, come $-[r]$ la classe $[-r]$ e come $[r]^{-1}$, se il resto della divisione di r per m *non* è 0, la classe $[r^{m-2}]$ (ciò è giustificato da un celebre teorema di Pierre Fermat, secondo cui se m è un numero primo non-divisore dell'intero m è $r^{m-1}\equiv 1$ mod m: dunque $r\cdot r^{m-2}=r^{m-1}\equiv 1$ mod m).

Oltre a un'articolata teoria delle congruenze – nel cui contesto Gauss dimostra rigorosamente il celebre principio dell'univocità della decomposizione in fattori primi degli interi – nelle *Disquisitiones* sono sviluppate altre idee fondamentali per la teoria dei numeri, quali le forme quadratiche (e la legge di reciprocità quadratica) e una trattazione abbastanza sistematica di quelli che oggi chiamiamo campi ciclotomici. Varrà inoltre la pena di ricordare che nella quinta sezione dell'opera viene ripresa la relazione di equivalenza tra forme quadratiche $ax^2+bxy+cy^2$ a coefficienti interi (con lo stesso discriminante b^2-4ac) introdotta a suo tempo da Lagrange (due forme sono equivalenti quando una di esse si deduce dall'altra con un cambiamento di variabili: $x'=\alpha x+\beta y$, $y'=\gamma x+\delta y$, ove α, β, γ, δ sono interi tali che $\alpha\delta-\beta\gamma=1$) e che per le corrispondenti classi di equivalenza viene introdotta una legge di composizione per la quale tali classi formano quello che oggi chiamiamo un gruppo abeliano. Nonostante l'analogia tra tale composizione e la moltiplicazione degli interi mod m con m primo, analogia che Gauss stesso segnala, per tale legge di composizione nelle *Disquisitiones* viene utilizzata la notazione additiva. «Questa indifferenza in fatto di notazioni testimonia una volta di piú la generalità che Gauss aveva certamente raggiunto nelle sue concezioni relative alle leggi di composizione» [Bourbaki 1960, trad. it. p. 70]. Aggiungiamo solo che, se pure Gauss non ebbe occasione di sviluppare sistematicamente idee che avrebbero potuto contribuire alla formazione di concetti fondamentali dell'algebra astratta, non mancano nella sua opera spunti in tale direzione. Valga come esempio la compatibilità, appunto, di una relazione di equivalenza con le operazioni in una struttura algebrica.

Per $m=2$ la teoria delle congruenze riprende un ordine di idee che risale almeno all'opposizione pari/dispari cara ai pitagorici: 'pari' e 'dispari' appaiono nomi per la classe [0] e per la classe [1] e le regole pitagoriche (l'unità è «pari/impari» perché aggiunta a un 'pari' dà un 'dispari', a un 'dispari' un 'pari'; 'pari' per 'pari' dà 'pari', 'dispari' per 'dispari' dà 'dispari', ecc.) si possono reinterpretare, scrivendo 0 e 1 per [0] e [1] rispettivamente, con le tabelle per l'addizione e la moltiplicazione nel sistema binario (cfr. § 2.1) ricordando che nella prima è $1+1=10$ ma 10 rappresenta il numero due che è appunto congruo a zero modulo due: il campo delle classi di resto mod 2 è quindi il corre-

lato formale rigoroso di quella aritmetica binaria che per Leibniz come in uno specchio forniva «l'immagine della creazione» [cit. in Courant e Robbins 1941, trad. it. p. 44] e che ci permette di individuare una nuova struttura, l'algebra di Boole a due elementi, che si rivela uno strumento essenziale per quella che chiameremo nel § 2.6 la tecnologia del pensare.

Dagli accenni alla teoria delle congruenze, vediamo subito che gli assiomi **I** non discriminano tra corpi con infiniti elementi (come il sistema dei razionali) e corpi con un numero finito di elementi (come i sistemi delle classi di resto mod m con m primo). Per un sistema assiomatico piú sottile ci basta constatare che i razionali – come i naturali e i relativi – possono venir ordinati dalla relazione $a \leq b$ che si legge «a è minore od uguale a b». In particolare il sistema dei razionali risulta un corpo ordinato, cioè un sistema **A** in cui è definita una relazione binaria $\leq$ tale che non solo **A** è un corpo commutativo, ma valgono anche gli assiomi:

II.1. Per ogni a, b, c di A, se $a \leq b$ e $b \leq c$, allora $a \leq c$
II.2. Per ogni a, b di A, $a \leq b$ e $b \leq a$ se e solo se $a = c$
II.3. Per ogni a, b di A, $a \leq b$ o $b \leq a$
II.4. Per ogni a, b, c di A, se $a \leq b$, allora $a + c \leq b + c$
II.5. Per ogni a, b di A, se $0 \leq a$ e $0 \leq b$, allora $0 \leq a \times b$.

Il lettore può osservare che II.5 è la piú semplice regola dei segni e può dedurre dagli assiomi anche le altre regole dei segni ricordate nel § 2.3. Diamo qui subito alcune definizioni che utilizzeremo nel seguito: in un corpo ordinato l'intervallo chiuso di estremi a, b, denotato con $[a, b]$, è l'insieme degli x tali che $a \leq x \leq b$; l'intervallo aperto, denotato (a, b), è invece l'insieme degli x tali che $a < x < b$ (ove la notazione $a < x$ significa $a \leq x$ e $a \neq x$).

Ricordiamo ancora che, in un corpo ordinato, intendiamo per valore assoluto di un elemento a (e scriviamo $|a|$) a stesso se $a \geq 0$, e $-a$ se $a < 0$.

Si può agevolmente verificare che anche altri sistemi, per esempio il sistema dei numeri reali (cfr. § 3.3), soddisfano gli assiomi I e II; ma l'aggiunzione degli assiomi II permette di escludere i corpi finiti e pone le premesse del discorso maggiorare/minorare/approssimare come vedremo meglio nel § 3.

2.5. Il calcolo di Boole.

Sono senza dubbio gli sviluppi dell'algebra (cfr. quanto detto nei §§ 2.3 e 2.4) che permettono di individuare calcoli con «entità» che non sono necessariamente numeri che forniscono un paradigma per gli stessi calcoli logici. Già in Leibniz è presente l'idea di una somiglianza tra disgiunzione e congiunzione di concetti da un lato e addizione e moltiplicazione di numeri dall'altro, anche se tale somiglianza non è formulata con precisione. È sostanzialmente nell'opera logica di George Boole che questo progetto trova piena attuazione. In Boole [1847 e ancor piú 1854] un calcolo, nel senso piú ampio del termine, viene caratterizzato come un metodo che si fonda sull'impiego di simboli, le cui leggi di combinazione sono «note» e «generali» e i cui risultati ammettono «globalmente» (cfr. § 2.7) un'interpretazione coerente. È questa idea, in particolare, che sottende l'enunciazione fatta da Boole del proprio programma: «Scopo di questo trattato è d'indagare le leggi fondamentali di quelle operazioni della mente per mezzo delle quali si attua il ragionamento; di dar loro espressione nel linguaggio simbolico di un calcolo e d'istituire, su questo fondamento, la scienza della logica costruendone il metodo; di fare, di questo stesso metodo, la base di un metodo generale per l'applicazione della dottrina matematica della probabilità e, in ultimo, di ricavare dai diversi elementi di verità portati alla luce nel corso di queste indagini alcune indicazioni probabili sulla natura e la costituzione della mente umana» [Boole 1854, trad. it. p. 9]. Qui non possiamo nemmeno accennare ai precedenti di tale progetto (l'algebra simbolica, la revisione del calcolo infinitesimale intesa soprattutto come svincolamento da tecniche «intuitive» e come generalizzazione sempre crescente dei metodi dimostrativi, il dibattito filosofico sulla natura della logica e della grammatica, ecc.) né delineare la realizzazione del programma nelle direzioni da Boole indicate [per tali tematiche rimandiamo a Bocheński 1956, Kneale 1962 e alla prefazione alla trad. it. di Boole 1854]; ci limitiamo a richiamare l'attenzione sul calcolo della logica, cioè sulla *logic of class* 'logica delle classi', che in via di principio Boole distingue dalla «filosofia di *tutto* il pensiero che sia esprimibile in segni, qualunque sia l'oggetto di quel pensiero» [cit. in Kneale 1962, trad. it. p. 463].

Supponiamo allora che lettere quali a, b, c, ... stiano ora non per quantità (come accade nel calcolo algebrico letterale) ma per classi: fungono – dice Boole – da «simboli elettivi» (*elective*), in quanto eleggono (cioè trascelgono) certe cose come oggetti d'attenzione e che l'uso del simbolo $=$ tra due simboli di classi indichi che le classi da tali simboli denotate hanno gli stessi membri (sono cioè coestensive). Tra tutte le classi distinguibili Boole segnala due casi-limite per cui introduce due appositi simboli 0 e 1, la classe universale (la classe della quale ogni cosa è membro) e la classe nulla (la classe della quale nessuna cosa è membro), con l'intesa che il segno 1 significhi ciò che nel suo *Formal Logic* [1847] De Morgan aveva chiamato *universe of discourse* 'universo del discorso', ossia non, genericamente, la totalità di tutti gli oggetti concepibili di qualsiasi genere, ma piuttosto la totalità di una determinata categoria di cose che sono oggetto della discussione (per esempio, in un contesto ove si suppone che i termini 'greco' e 'straniero' determinino due classi complementari, l'universo del discorso è il genere umano [De Morgan 1847, p. 55]): felice prudenza, dato che – come ben ci si accorse nella controversia sui fondamenti della matematica agli inizi del Novecento – l'uso senza restrizione della nozione di classe universale porta ad antinomie logiche.

Ma vediamo le operazioni di questo calcolo: innanzitutto Boole richiama l'attenzione sulla intersezione o moltiplicazione di due classi a, b (cioè sulla classe di tutte le cose che appartengono sia ad a che a b), che indicheremo con il simbolo $a \times b$ che per certe proprietà rimanda alla moltiplicazione dei numeri. Proprio dal confronto con l'usuale calcolo dei numeri Boole pone il problema

se anche nel calcolo della logica si possa definire l'operazione inversa; pur constatando che dall'equazione $ab = cb$ non si ricava l'equazione $a = c$ (la classe degli arcidiaconi celibi può forse essere coestesa alla classe degli arcidiaconi biondi, ma da ciò non segue che tutti i celibi siano biondi), Boole non abbandona la funzione euristica dell'analogia coi calcoli piú familiari, dato che anche nell'algebra numerica vi sono limiti proprio nell'uso dell'operazione di divisione (da $2 \times 0 = 3 \times 0$ non possiamo passare all'equazione $2 = 3$).

Nell'algebra delle classi il segno $a+b$ denota la classe delle cose appartenenti *o* alla classe denotata da a *o* alla classe denotata da b: la parola 'o' verrà intesa qui, salvo avviso contrario, sempre in senso inclusivo (in questa accezione nella classe degli uomini che sono greci *o* biondi rientrano anche quegli uomini che sono greci *e* biondi). Presentiamo ora una versione delle leggi (che hanno per il calcolo della logica la stessa funzione che avevano quelle elencate nel § 2.4 per il calcolo coi razionali) un po' diversa da quella originale di Boole [1854]. Si tratta sostanzialmente di un riadattamento di Edward V. Huntington [1904, pp. 288-309] di un'idea contenuta nella *Universal Algebra* di Whitehead [1898].

Per «algebra di Boole» intendiamo dunque un sistema **B** costituito da un insieme B, dalle due applicazioni binarie a un solo valore $+$ e $\times$ di $B \times B$ in B, da un'applicazione a un solo valore $'$ di B in B e da due elementi specifici distinti di B, 0 e 1, in modo che valgano gli assiomi:

1. *a*)	Per ogni a, b in B,	$a+b=b+a$	proprietà commutativa
b)	Per ogni a, b in B,	$a \times b = b \times a$	
2. *a*)	Per ogni a, b, c in B,	$(a+b)+c = a+(b+c)$	proprietà associativa
b)	Per ogni a, b, c in B,	$(a \times b) \times c = a \times (b \times c)$	
3. *a*)	Per ogni a, b, c in B,	$a+(b \times c) = (a+b) \times (a+c)$	proprietà distributiva
b)	Per ogni a, b, c in B,	$a \times (b+c) = (a \times b)+(a \times c)$	
4. *a*)	Per ogni a in B,	$a+0=a$	
b)	Per ogni b in B,	$a \times 1 = a$	
5. *a*)	Per ogni a in B,	$a+a'=1$	
b)	Per ogni a in B,	$a \times a' = 0$.	

Si nota immediatamente che gli assiomi sono formulati in modo da mettere in risalto il cosiddetto principio di dualità: se una proposizione è derivabile dagli assiomi 1-5 la proposizione duale (ove $+$ è sostituito da $\times$, $\times$ da $+$, 0 da 1 e 1 da 0) è derivabile da 1-5. Inoltre un'indagine piú attenta mostra che in questa formulazione *non* tutti gli assiomi sono indipendenti: alcuni sono ricavabili dagli altri e solo per maggior chiarezza sono stati elencati qui [per una versione degli assiomi che evidenzia l'indipendenza di ogni postulato cfr. Kneale 1962, trad. it. p. 482]. Ciò premesso, mostriamo come possiamo derivare «formalmente» (senza cioè sfruttare alcuna interpretazione degli assiomi) la legge $a \times a = a$ che per George Boole individuava la specificità del proprio calcolo in quanto indicava la piú vistosa differenza dall'ordinaria algebra dei numeri.

La derivazione sarà qui intenzionalmente eseguita non solo senza tralasciare alcun passaggio ma addirittura giustificando anche quelli apparentemente banali, dato che lo scopo del calcolo, nell'accezione di questo paragrafo, non è quello di persuadere della «verità» di un risultato, ma di mettere in evidenza la struttura dell'inferenza dalle premesse alle conclusioni. Abbiamo dunque:

$a+a'=1$	(per 5*a*).
$a \times (a+a') = a \times 1$	(l'applicazione $\times$ è a un solo valore)
$a \times a + a \times a' = a \times 1$	(per 3*b*).
$a \times a + 0 = a \times 1$	(per 5*b*).
$a \times a = a \times 1$	(per 4*a*).
$a \times a = a$	(per 4*b*).

L'ultimo anello della catena deduttiva esprime appunto per il caso $n=2$ la legge che Boole chiama *the index law*

$$a^n = a \qquad \text{cioè} \quad \underbrace{a \times \ldots \times a}_{n \text{ volte}} = a;$$

una legge analoga

$$na = a \qquad \text{cioè} \quad \underbrace{a + \ldots + a}_{n \text{ volte}} = a$$

vale per l'addizione (per $n=2$ possiamo ottenerla dalla derivazione precedente per dualità).

L'antitesi forma/interpretazione si delinea con chiarezza: già le considerazioni di «dualità» rimandano piú alla manipolazione dei simboli che a una loro interpretazione. Ciò era ben presente a Boole che cosí scriveva nell'*Analysis of Logic* [1847]: «Coloro che hanno familiarità con lo stato attuale della teoria dell'algebra simbolica, sono consapevoli che la validità dei procedimenti dell'analisi non dipende dall'interpretazione dei simboli che vi sono impiegati, ma soltanto dalle leggi che regolano la loro combinazione. Ogni sistema di interpretazione che non modifichi la verità delle relazioni che si suppone sussistano tra tali simboli è egualmente ammissibile, ed è cosí che il medesimo processo può, secondo uno schema d'interpretazione, rappresentare la soluzione di una questione riguardante le proprietà dei numeri, secondo un altro schema quella di un problema di geometria, e, secondo un altro ancora, quella di un problema di dinamica o di ottica» (trad. it. pp. 51-52). Per illustrare tale considerazione, limitiamoci alle «proprietà dei numeri». Prendiamo per B l'insieme dei naturali che sono divisori di 70, cioè $\{1, 2, 5, 7, 10, 14, 35, 70\}$: per $a \times b$ intendiamo il MCD (massimo comun divisore) di a e b, per $a+b$ il loro MCM (minimo comune multiplo), per a' infine $70/a$, per 1 e 0 rispettivamente 70 e 1: il lettore può agevolmente verificare che abbiamo ottenuto un sistema per cui valgono gli assiomi di Whitehead e Huntington, cioè un'algebra di Boole: stavolta '$+$' e '$\times$' indicano operazioni tra numeri, ma non gli usuali $+$ e $\times$, bensí le operazioni che determinano MCM e MCD di due numeri, ecc.

Prima di concludere questo paragrafo mostriamo ancora come l'ordine di idee introdotto da Boole permette di interpretare come un particolare calcolo

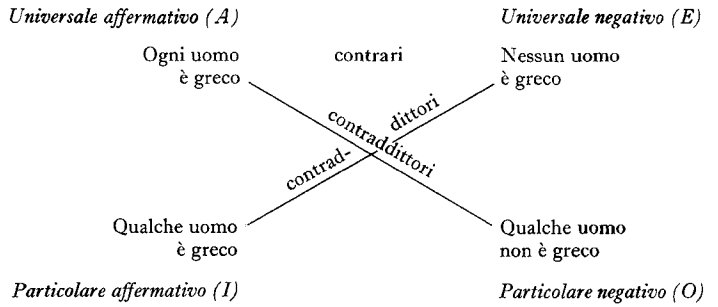


Figura 7.

Lo schema del quadrato logico, illustrato con un esempio tratto da Aristotele. La notazione booleana descritta in questo paragrafo è sufficiente ad esprimere le proposizioni A, E, I, O purché le proposizioni A ed E siano prese senza portata esistenziale, come venne mostrato da Franz Brentano nella *Psychologie vom empirischen Standpunkt* (1874). La lettera u sta per la classe degli esseri umani, la lettera g per la classe dei Greci. A, E, I, O possono essere allora espresse rispettivamente dalle formule $u \times g' = 0$ (o anche $u \times g = g$), $u \times g = 0$, $u \times g \neq 0$, $u \times g' \neq 0$.

la sillogistica aristotelica. Per esempio (cfr. fig. 7) il sillogismo in B*A*RB*A*R*A* può venir trattato cosí: u stia per la classe degli esseri uomini, a per la classe degli animali, m per la classe dei mortali; le premesse 'Ogni essere umano è un animale' e 'Ogni animale è mortale' possono venir rimpiazzate per esempio dalle equazioni:

(1) $u+a=a$

(2) $a+m=m$

e quindi sostituendo nella (2) l'espressione per a data dalla (1) otteniamo:

(3) $(u+a)+m=m$ (l'applicazione + è a un sol valore)

(4) $u+(a+m)=m$ (per 2*a*)

e usando ancora la (2)

(5) $u+m=m$

che il lettore può, se vuole, trasformare agevolmente in:

(6) $u \times m' = 0$.

(5) ovvero (6) possono appunto venir interpretate come 'Ogni essere umano è mortale'.

2.6. Algebra a due valori. Calcolo proposizionale. Circuiti logici.

L'interesse delle derivazioni formali del § 2.5 non è puramente teorico; risiede anche nel fatto che i metodi introdotti da Boole che abbiamo visto alla

prova sulla *index law* come sulla sillogistica aristotelica sono, per cosí dire, «applicabili meccanicamente».

Per chiarire questa locuzione premetteremo qualche cenno sull'algebra a due valori, su un importante teorema del calcolo booleano e sul calcolo proposizionale, limitandoci a una esposizione informale e inviando il lettore per esempio a Mendelson [1964] per ulteriori particolari.

Il corpo delle classi di resto mod 2 che abbiamo già visto nel § 2.4 si trasforma immediatamente in un'algebra di Boole interpretando il prodotto di due classi come prodotto logico, definendo la somma logica per a, b nel corpo come $(a+b)-(a \times b)$ ove + e × sono definiti come nel § 2.4 e prendendo come 0 e 1 booleani [0] e [1] rispettivamente e infine $[0]' = [1]$ e $[1]' = [0]$.

In tale algebra «i simboli a, b, c, ecc. ammettono indifferentemente i valori 0 e 1 e solo questi» [Boole 1854, trad. it. p. 60].

Chiamiamo ora espressione booleana ogni espressione ricavata dai simboli a, b, c, ... applicando le operazioni booleane +, ×, ′ un numero finito di volte. In altre parole 1) tutte le lettere a, b, c, ... sono espressioni booleane; 2) se τ e σ sono espressioni booleane tali sono anche $\sigma+\tau$, $\sigma \times \tau$, τ'; 3) sono espressioni booleane solo quelle espressioni determinate da 1) e da 2). In particolare indichiamo con $\tau\ (a_1, ..., a_k)$ una espressione costruita con le k lettere $a_1, ..., a_k$. Un importante teorema garantisce allora che τ può scriversi come τ^* somma di prodotti di espressioni dell'insieme $\{a_1, ..., a_k, a_1', ..., a_k'\}$ dove al solito con a_i' denotiamo il complemento di a_i; si dice pure che τ^* è una forma normale disgiuntiva di τ. Da esso segue [Mendelson 1970, trad. it. p. 62] che un'uguaglianza se vale per un'algebra booleana, in particolare per un'algebra a due elementi, vale per tutte le algebre booleane.

Ciò premesso, diamo qualche cenno al calcolo delle proposizioni. Ci limitiamo a considerare proposizioni «composte» la cui verità o falsità risulti determinata dalla verità o falsità delle proposizioni che concorrono a formarle. Con 1 e 0 indicheremo ora convenzionalmente i valori di verità 'vero' e 'falso' rispettivamente.

La negazione ('non') è una delle operazioni piú semplici sulle proposizioni: se A è una proposizione, con $\neg A$ denotiamo la negazione di A che caratterizziamo con la seguente tavola di verità:

A	$\neg A$
1	0
0	1

Altre operazioni su proposizioni sono la congiunzione ('e'), la disgiunzione inclusiva ('o') che per proposizioni A, B denoteremo rispettivamente $A \& B$, $A \vee B$ e che caratterizzeremo con le seguenti tavole di verità:

A	B	$A \& B$	$A \vee B$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	0

Chiamiamo ora forma proposizionale ogni espressione ricavata dai simboli A, B, C, ... applicando le operazioni $\vee$, &, $\neg$ un numero finito di volte, in altre parole 1) tutte le lettere A, B, C, ... sono forme proposizionali; 2) se **S** e **T** sono forme proposizionali allora lo sono anche **S** & **T**, **S** $\vee$ **T**, $\neg$**S**; 3) forme proposizionali sono solo quelle definite in 1) e 2).

Ciò premesso, è ovvio che l'assegnazione di valori di verità 1 oppure 0 a ogni lettera che compare in una forma proposizionale fa corrispondere un valore di verità per la forma proposizionale che può venir «calcolato» utilizzando un'opportuna tavola di verità che possiamo costruire servendoci delle tavole date sopra. Possiamo anche dire che una qualsiasi forma proposizionale determina una funzione di verità, cioè un'applicazione di $\{0, 1\}^n$ in $\{0, 1\}$ ove n è il numero delle lettere che compaiono nella forma proposizionale. In particolare chiameremo logicamente equivalenti forme proposizionali che determinano la stessa funzione. Una conseguenza di un profondo teorema, che riprende un'idea di Peirce (Sheffer, 1913), assicura che ogni funzione di verità, cioè ogni applicazione di $\{0, 1\}^n$ su $\{0, 1\}$ per n qualsiasi, può a sua volta venir determinata da una forma proposizionale in cui occorrono solo i connettivi $\neg$, $\vee$, oppure solo i connettivi $\neg$, & (il teorema di Sheffer è piú forte: a rigore è sufficiente un opportuno connettivo, come la doppia negazione di Sheffer, ma per i nostri scopi basta quanto abbiamo detto).

È immediato ora scorgere l'affinità dei due calcoli (proposizionale e delle classi). Possiamo infatti tradurre espressioni booleane in forme proposizionali e viceversa, facendo corrispondere alle lettere a, b, c, ... le lettere A, B, C, ..., ai segni booleani $+$, $\times$, $'$ i connettivi $\vee$, &, $\neg$ (sicché le tabelle riportate sopra caratterizzano quindi anche la moltiplicazione e il prodotto logico che abbiamo introdotto nel § 2.5), allo 0 e all'1 booleani le proposizioni $\neg A \& A$ («legge di contraddizione») rispettivamente $\neg A \vee A$ («terzo escluso»). σ e τ siano allora due espressioni booleane e **S** e **T** le corrispondenti forme proposizionali; per vedere se **S** e **T** determinano la stessa funzione di verità basta ricorrere alle tavole di verità: dai teoremi sopra ricordati segue subito che $\sigma = \tau$ se e solo se **S** e **T** sono logicamente equivalenti.

Le tavole di verità permettono dunque di decidere in un numero finito di passi l'uguaglianza di due espressioni booleane come l'equivalenza logica di due forme proposizionali. È in questo senso che i metodi di Boole sono riducibili a regole meccaniche e come tali rimandano a quella che in modo forse non del tutto esatto ma pregnante è stata chiamata «la tecnologia del pensare» con esplicito riferimento al progetto booleano di studiare *the laws of thought* 'le leggi del pensiero' [Boole 1854].

È stato Jevons il primo a intuire un fatto del genere e a costruire nel 1869 una macchina logica, presentata l'anno successivo alla Royal Society, macchina che egli stesso assimila a un piccolissimo piano verticale. «Noi la paragoneremmo piuttosto a un registratore di cassa, poiché i segni che indicano le varie combinazioni possibili di elementi (siano queste classi o proposizioni) son fatti apparire e sparire premendo tasti» [Kneale 1962, trad. it. p. 479]. Nel 1885 Allan Marquand progetta un *analogon* elettrico della macchina di Jevons; ma è nel 1947 che il progetto trova piena attuazione, sfruttando una tecnologia piú sofisticata: il calcolatore costruito a Harvard da Kalin e Burkhart è in grado di risolvere problemi booleani in cui intervengono sino a dodici variabili logiche, cioè dodici lettere proposizionali o lettere di classi.

L'antitesi forma/interpretazione ci ripropone quella astratto/concreto. Cominciamo col passare dalle generalissime «leggi del pensiero» allo studio dei circuiti di commutazione. In seguito alla memoria di Shannon (1938) un circuito elettrico contenente solo interruttori a due posizioni (quando l'interruttore è chiuso passa la corrente, quando è aperto no) viene rappresentato da uno schema in cui, vicino a ogni interruttore, si pone una lettera che rappresenta una proposizione tale che l'interruttore è chiuso quando la proposizione è vera ed è aperto quando è falsa. La condizione di passaggio della corrente attraverso l'intero circuito è dunque rappresentabile con una forma proposizionale (si veda per un esempio la figura 8).

Una volta «concretizzata» l'algebra booleana come algebra dei circuiti di commutazione, è agevole la trattazione dei problemi booleani: per esempio, certi aspetti dell'articolazione logica dell'ordinario calcolo coi numeri su un calcolatore digitale.

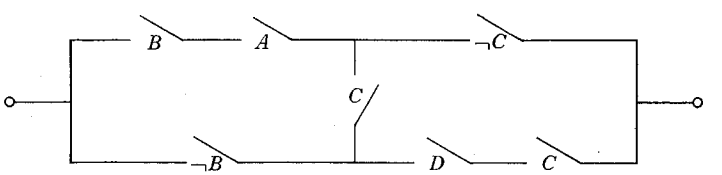


Figura 8.

Il circuito viene rappresentato dalla forma proposizionale $(A \& B \& C \& D) \vee (A \& B \& \neg C) \vee (\neg B \& C \& D)$ che si può ottenere cercando tutte le plausibili vie attraverso il circuito. Si osservi che la via da $\neg B$ a $\neg C$ attraverso C non viene presa in considerazione, in quanto essa darebbe la congiunzione elementare $\neg B \& C \& \neg C$ logicamente falsa. Al circuito viene cosí associata una funzione di verità.

A tale strumento tocca infatti un importante ruolo di elaborazione dell'informazione e proprio a questo scopo si realizzano i cosiddetti *blocchi logici elementari*.

Per esempio un blocco AND è un dispositivo che opera su $n \geq 2$ «entrate» $A_1, \ldots, A_n$ cioè su n grandezze fisiche in cui si distinguono due *stati* indicati al solito con 0 e 1: lo stato 1 si determina quando A_i $(1 \leq i \leq n)$ è vera, e lo stato 0 quando A_i è falsa. La «uscita» AND ha solo due possibili stati 0 e 1: è 1 se e solo se $A_1 \& A_2 \& \ldots \& A_n$ è vera, è 0 se e solo se $A_1 \& A_2 \& \ldots \& A_n$ è falsa. Dal punto di vista astratto l'uscita di AND non è altro che il prodotto logico delle entrate e per $n=2$ può venir caratterizzata dalla tavola di verità di & nella tabella a p. 402.

Un altro blocco è l'OR. Se le entrate sono $A_1, \ldots, A_n$ $(n \geq 2)$, l'uscita è $A_1 \vee A_2 \vee \ldots \vee A_n$: cioè, dal punto di vista astratto, la *somma logica* inclusiva delle entrate e per $n=2$ può venir caratterizzata dalla tavola di verità di $\vee$ nella stessa tabella.

Infine il blocco NOT è un dispositivo che ha un'entrata A e produce un'uscita $\neg A$: l'uscita di NOT può dunque venir caratterizzata dalla tavola di verità di $\neg$ nella tabella a p. 401.

Possiamo ora definire i circuiti logici combinatori appunto come combinazioni di blocchi tipo AND, OR, NOT: sotto il profilo astratto ci basta anche meno di AND e OR (per due entrate) e di NOT (cfr. quanto detto sopra a proposito del teorema di Sheffer: ovviamente è possibile anche un blocco a due entrate NAND che corrisponde alla doppia negazione di Sheffer). Per un esempio si veda la figura 9.

Ma riprendiamo l'ottica astratto/concreto/astratto: per attuare una data funzione di verità sono possibili, come si è visto, piú circuiti in astratto logicamente equivalenti e la possibilità di scelta conduce allora alla ricerca del circuito «ottimale». Orbene la determinazione di cosa sia ottimale può differire da tecnologia a tecnologia e da utilizzazione a utilizzazione. Poiché diversi fattori sono da tenersi in conto nella definizione (costo, affidabilità del circuito realizzato, rapidità della risposta, ecc.), un circuito ottimale non può che rappresentare un compromesso tra tali fattori quando si dia a ciascuno di essi un peso diverso in relazione alle diverse utilizzazioni. Tale mediazione è di nuovo un passo verso l'astratto: tecniche di progetto ottimali si dànno solo relativamente a specifiche definizioni di ottimalità. Ma la ineliminabile componente convenzionale di una definizione formale di cos'è ottimale non è indice di ricerca sterile. Per esempio possiamo assumere che il fattore di maggior rilievo sia quello relativo alla rapidità di risposta del circuito e che il solo altro fattore che deve essere tenuto in conto sia quello relativo al numero dei blocchi, prescindendo dalla considerazione di elementi NOT dato che la presenza o l'assenza del segno di negazione risulta spesso da una decisione arbitraria (di qui la convenzione di considerare le negazioni delle lettere come entrate iniziali e di non contare i blocchi NOT tra gli elementi del circuito). Dalla prima asserzione deriva la richiesta che il circuito sia a due stadi (un segnale che si trasferisca dall'ingresso all'uscita non deve cioè attraversare piú di due blocchi),

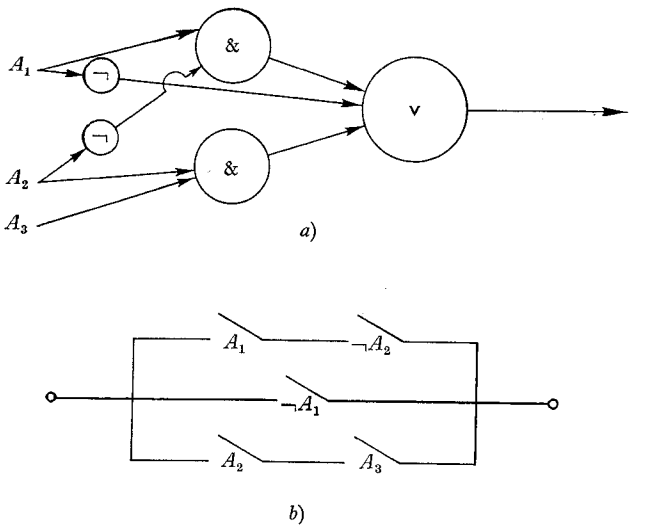


Figura 9.

In *a*) è raffigurato un circuito logico per $(A_1 \& \neg A_2) \vee \neg A_1 \vee (A_2 \& A_3)$ che adopera i blocchi NOT, OR, AND simbolizzati con $\neg$, &, $\vee$ rispettivamente. In *b*) è raffigurata una serie di circuiti di commutazione serie-parallelo in cui la corrente passa se e solo se la formula in questione è vera: il collegamento in serie corrisponde all'AND, quello in parallelo all'OR.

il che mette in risalto l'importanza delle forme normali disgiuntive che tale esigenza soddisfano. La seconda pone un problema di minimizzazione dei blocchi, cioè il problema di determinare una forma normale disgiuntiva logicamente equivalente a una data forma proposizionale A e tale che nessun'altra forma normale disgiuntiva piú semplice sia ad A logicamente equivalente. E infine l'esigenza pratica si riconnette a rilevanti sviluppi teorici: metodo di Quine e McCluskey, mappe di Karnaugh, ecc. ciascuno coi rispettivi vantaggi e svantaggi. Per tali metodi rimandiamo il lettore interessato a Mendelson [1970]: qui abbiamo voluto piuttosto dare un esempio della non semplice dialettica inerente al problema dell'*ottimizzazione* di certe procedure, un problema che avremo modo di riprendere in altro contesto.

2.7. Calcolo logico e concetto astratto di calcolo.

Quegli elementi che abbiamo isolato nella concettualizzazione di Boole e negli sviluppi a questa connessi – calcolo delle proposizioni, funzioni di verità, forme normali disgiuntive – nella direzione indicata da parole come 'calcolatore', 'macchina', 'tecnologia' assumono rilevanza anche nella direzione apparentemente opposta, quella cui rimandano termini come 'metodo assiomatico', 'linguaggio perfetto', 'sistema formale'.

Non è minimamente possibile accennare, in quest'ottica, ai grandi sviluppi della logica da Boole agli anni '30 del Novecento. Basteranno poche citazioni: nella *International Encyclopedia of Unified Science* l'analisi dei fondamenti logici delle scienze muove dalla premessa che «un *calcolo K* è un sistema di regole formali che consiste di una *classificazione* dei segni, di *regole di formazione* (che definiscono le formule di *K*) e di *regole di deduzione*. Le regole di deduzione consistono di solito in enunciati primitivi ed in regole di inferenza (che definiscono "direttamente derivabile in *K*"). Talvolta *K* contiene anche regole di refutazione (che definiscono "direttamente refutabile in *K*"). Se *K* contiene definizioni queste possono venir considerate come regole addizionali di deduzione» [Carnap 1942, p. 155]. Sotto un certo profilo dietro Carnap riemerge Leibniz, dietro Leibniz, Hobbes (cfr. § 1), ma attraverso la mediazione non solo dell'«algebra della logica» ma anche delle «grandi logiche» progettate da Frege e quindi da Russell e Whitehead. Senza contare che la caratterizzazione puramente *sintattica* della deduzione (per Carnap stesso 'calcolo' è sinonimo di *syntactical system* o di *formal system* [1942, pp. 155 sgg.]) è presente nelle indagini oramai classiche di Hilbert sui fondamenti della geometria (1899-1900) e si puntualizza nelle meticolose analisi promosse dai formalisti della «scuola di Hilbert» negli anni '20 e '30. Ed è a questa tradizione che si riconnette l'idea del «calcolo logico» in generale come «rappresentazione di un sistema deduttivo eseguita in modo tale che a ciascun principio di deduzione corrisponda una regola di *manipolazione* dei simboli» [Braithwaite 1953, trad. it. p. 27]. Il rigore matematico diventa cosí rigore formale: se Poincaré [1902] ammoniva matematici e fisici-matematici a guardarsi dal servirsi di *hypothèses cachées* nei loro ragionamenti, in Braithwaite [1953] c'è un passo ulteriore: «L'uso del calcolo per rappresentare un sistema deduttivo presenta l'enorme vantaggio pratico di rendere possibili deduzioni effettuate unicamente mediante manipolazioni di simboli e la correttezza di queste deduzioni può essere controllata automaticamente [*checked automatically*] con la mera verifica delle relazioni tra i simboli», sicché con sguardo all'indietro (cfr. § 2.1) si può concludere che «se è per questa ragione che l'invenzione indiana dei numeri "arabi" fu un evento cosí decisivo nella storia della civiltà... l'uso del calcolo garantisce [a sua volta] che il pensiero venga completamente esplicitato, poiché nessun principio di deduzione può essere usato nel sistema deduttivo che non sia rappresentato da una regola di manipolazione simbolica del calcolo» [Braithwaite 1953, trad. it. p. 27].

Per dare un'idea piú precisa del calcolo in questa accezione basta vedere in qualunque buon manuale di logica [per esempio Mendelson 1964] le presentazioni del calcolo proposizionale, del calcolo dei predicati del primo ordine senza/con identità, del calcolo dei predicati di ordine superiore, ecc. Il lettore stesso può interpretare la presentazione del calcolo delle proposizioni data nel § 2.6 come una descrizione – ancora piuttosto informale – di un particolare calcolo *K*. Nel § 2.6 abbiamo classificato dei simboli, abbiamo fornito delle regole di formazione (cosí infatti possono venir interpretate la definizione di forma proposizionale qualora si autorizzi a rimpiazzare con proposizioni le

lettere proposizionali). Possiamo ora ricavare gli enunciati primitivi sostituendo proposizioni alle lettere proposizionali in ciascun elemento di un insieme finito di schemi di assiomi come quello proposto da Russell e Whitehead [1910], ove si utilizzano solo i due connettivi $\neg$, $\vee$:

R.1. $\neg(\mathbf{A}\vee\mathbf{A})\vee\mathbf{A}$
R.2. $\neg\mathbf{B}\vee(\mathbf{A}\vee\mathbf{B})$
R.3. $\neg(\mathbf{A}\vee\mathbf{B})\vee(\mathbf{B}\vee\mathbf{A})$
R.4. $\neg(\neg\mathbf{B}\vee\mathbf{C})\vee(\neg(\mathbf{A}\vee\mathbf{B})\vee(\mathbf{A}\vee\mathbf{C}))$

Tale sistema è riportato qui seguendo le usuali convenzioni sulle parentesi. Oltre alla naturale regola di sostituzione l'unica regola di deduzione è il classico *modus ponendo ponens*: possiamo inferire **B** da **A** e $\neg\mathbf{A}\vee\mathbf{B}$.

Calcoli piú sofisticati, per esempio il calcolo dei predicati del primo ordine, in genere, non sono «meccanici» nel senso del § 2.6: non possono venir ridotti, cioè, a tavole di verità o a qualche altra procedura effettiva. In generale per un calcolo *K* si richiede che siano effettivi i metodi di controllo [Mendelson 1964, trad. it. p. 42], che cioè si possa decidere, in un numero finito di passi, se siamo di fronte a un'espressione di *K*, cioè a una sequenza finita di segni di *K*, a una formula di *K*, a un assioma di *K* e se, data una sequenza finita di formule di *K*, ciascuna di queste sia un assioma o sia ottenuta dagli assiomi applicando una delle regole di deduzione di *K*. Dunque non sempre possiamo effettivamente decidere se una formula di *K* è un teorema di *K*, se cioè esiste una derivazione formale di tale formula in *K*; possiamo però decidere effettivamente se una data successione che termina con una certa formula è una derivazione formale oppure no.

Il concetto astratto di calcolo testé caratterizzato ridefinisce in un modo singolare l'antica idea del calcolo come «arte» o come «gioco». Whitehead [1898, p. 4]: «Una volta note le regole per la manipolazione dei segni del calcolo, l'arte della loro manipolazione pratica può venir studiata prescindendo dall'attenzione al significato assegnato ai segni. È ovvio che possiamo prendere tutti i contrassegni [*marks*] che vogliamo e manipolarli secondo regole che assegnamo a nostra scelta». Ma convenzionalismo matematico ed economia di pensiero vanno di pari passo: là dove diversi sistemi di oggetti, «pur determinati da differenti proprietà» dànno origine alle stesse «*notae* caratteristiche», vengono cioè analizzati con calcoli analoghi dal punto di vista formale anche se differenti per la scelta dei contrassegni [*ibid.*, p. 1], è «facile» tradurre un testo nell'altro. Ciò avviene abitualmente per le teorie algebriche, ove un sistema di assiomi è soddisfatto da un numero indefinito di sistemi di oggetti – cioè, come diciamo piú abitualmente, di strutture – anche notevolmente diverse: ricordiamo, per esempio, la teoria generale dei corpi commutativi (cfr. § 2.4) e quella delle algebre di Boole (cfr. § 2.5).

Traduzioni non banali sono infatti possibili anche con calcoli a prima vista molto meno «astratti». Riprendiamo l'esempio di Carnap [1939] concernente la teoria dei numeri naturali di Peano-Dedekind e la teoria dei numeri cardinali

finiti [trattata per esempio in Russell e Whitehead 1910]. Il primo è inteso come esempio di calcolo matematico che ammette tra gli enunciati primitivi oltre agli assiomi di un opportuno calcolo logico con identità anche specifici assiomi non di tipo logico; il secondo è inteso invece come un frammento di un calcolo logico superiore, conformemente alla concezione logicista.

Negli assiomi di Dedekind-Peano compaiono i segni primitivi specifici b, N, $*$:

P.1. b è un N.

P.2. Per ogni x, se x è un N, allora x^* è un N.

P.3. Per ogni x, se x è un N e y è un N e $x^*=y^*$, allora $x=y$.

P.4. Per ogni x, se x è un N, allora $b \neq x^*$.

P.5. Per ogni F [se b è un F e per ogni x (se x è un F allora x^* è un F)] allora per ogni y (se y è un N, allora y è un F).

Nell'interpretazione abituale b designa il numero 0, se '...' designa un numero naturale n, allora '...*' designa $n+1$ e N designa l'insieme dei naturali; ma se, per esempio, sostituiamo a 0, n, $n+1$, insieme dei numeri naturali, rispettivamente 2, $2n$, $2n+2$, insieme dei numeri pari maggiori di 0, anche questa interpretazione soddisfa gli assiomi P.1-P.5. Carnap [1939] sostituisce ai segni primitivi b, $*$, N rispettivamente 0, $^+$, 'numero cardinale finito':

P'.1. 0 è un numero cardinale finito.

P'.2. Per ogni m, se m è un numero cardinale finito, allora m^+ è un numero cardinale finito.

P'.3. Per ogni m, n, se m è un numero cardinale finito e n un numero cardinale finito e $m^+=n^+$, allora $m=n$.

P'.4. Per ogni m, se m è un numero cardinale finito, allora $0 \neq m^+$.

P'.5. Per ogni H [se 0 è un H e per ogni m (se m è un H allora m^+ è un H)] allora per ogni n (se n è un numero cardinale finito allora n è un H).

Per il logicista in questo modo l'aritmetica è ricondotta alla logica ed è determinato univocamente il significato dei numeri naturali; ma non entriamo qui in merito alle difficoltà di questo punto di vista [per cui cfr. Waismann 1936, trad. it. pp. 126 sg.]. Piuttosto osserviamo che senza che nemmeno gli sia richiesto di conoscere il significato di 0, $^+$, 'numero cardinale finito', il lettore può cogliere immediatamente le «caratteristiche formali» comuni a P.1-P.5 e a P'.1 - P'.5. Se si entra in quest'ottica, «un calcolo, in sé, non richiede alcuna giustificazione» [Carnap 1939, p. 20]. «Considerato isolatamente, senza un'interpretazione qualsiasi, è una partita fatta per un solo giocatore e giocata con segni tracciati sulla carta... L'apparato del gioco consiste di un foglio di carta rigato da linee orizzontali, con certi segni, o sequenze di segni, già tracciati sulle prime righe. Ciascuno di questi segni, o di questa sequenza di segni, verrà chiamato formula, laddove "formula" sta appunto per il segno o sequenza di segni scritti su una riga. Le formule che il giocatore trova scritte nel foglio

prima che egli cominci a giocare saranno chiamate *formule primitive*. Le regole del gioco sono le istruzioni date al giocatore su come egli possa scrivere nuove formule sul foglio di carta; ciascuna delle nuove formule viene derivata da alcune o da tutte quelle precedenti secondo le regole del gioco. Se chiamiamo lo scrivere una nuova formula *fare una mossa*, giocare consisterà nel fare una serie di mosse secondo le regole» [Braithwaite 1953, trad. it. p. 29]. Il senso del linguaggio «logicamente perfetto», cioè artificiale e non-ambiguo, dalla grammatica rigorosamente specificata si unisce alla caratterizzazione delle teorie come «sistemi ipotetico-deduttivi» (Pieri, Peano, ecc.) e a quella piú sofisticata come sistemi assiomatico-formali (Hilbert). Il problema dell'interpretazione di un «calcolo» o di un «testo» in questa particolare accezione porta alla coppia sintassi/semantica [Carnap 1942].

Ma questo raffinarsi della dicotomia forma/contenuto in *una* forma / *piú* interpretazioni può essere ancora una volta riletto nell'ottica dell'opposizione essenzialismo/nominalismo. Occorre non andar oltre la definizione rigorosa delle regole con cui si manipolano i simboli? «Nel gioco degli scacchi non interessa conoscere o definire l'essenza dei vari pezzi, ma conoscerne o definirne le regole... il cavallo si identifica perfettamente con il modo che esso ha di muoversi sulla scacchiera» [Frola e Miranda 1941, p. 259]. Ma alle forme piú o meno sofisticate di convenzionalismo si può ribattere che progettare un calcolo matematico come un «gioco» cui «non è connesso pensiero» è diverso dal prescindere per scopi particolari (cfr. per esempio § 5.3) dal significato di un calcolo nella pratica matematica. Quel che l'ottica «nominalista» non vede è che la concezione astratta dei calcoli permette «una riproduzione della [pratica matematica] nel piano del *formale puro*» [Waismann 1936, trad. it. p. 93]; quel che la concezione «essenzialista» non intende è invece che tale «riproduzione» non pretende di fornire l'esatta copia o tanto meno di esaurire la pratica matematica stessa.

2.8. Macchine calcolatrici e automi finiti.

Siamo rimandati quindi alla coppia astratto/concreto e tralasciando due immagini entrambe fortemente riduttive del calcolo, esemplifichiamo approfondendo quanto detto nel § 2.6 sui circuiti di commutazione. Essi possono venir intesi, seguendo Church (1957), come automi deterministici finiti. Tali automi sono caratterizzati in generale da un numero finito n di entrate $E_1, \ldots, E_n$, un numero finito di uscite $U_1, \ldots, U_n$ e ancora di un numero finito p di elementi interni $L_1, \ldots, L_p$: ciascuno di questi «elementi» (entrate, elementi interni, uscite) è capace di un certo numero di stati, diciamo due, per considerare solo automi binari; inoltre è data una scala del tempo $t=0, 1, 2, \ldots$ e in ogni istante ogni elemento si trova esattamente in uno dei suoi stati. Gli stati $S(E_i, t)$ delle entrate vengono assegnati dall'esterno e gli stati $S(U_k, t)$ vengono quindi prodotti «automaticamente» dalla «macchina».

Supponiamo, per semplicità, che sia $n=1$ come nei casi presentati nel § 2.6 e consideriamo per esempio il comportamento di NOT: è $S(U, t)=1$ se

e solo se $S(E, t) = 0$. Cosí la logica dei predicati a un posto, in cui riusciamo a esprimere che 'x ha la proprietà P' scrivendo $P(x)$ ove P è appunto un predicato a un posto, e addirittura che 'ogni x ha la proprietà P' o che 'esiste un x che ha una proprietà P' cioè $\forall x P(x)$, $\exists x P(x)$ rispettivamente, sembra l'ambito piú naturale (ricordiamo che $\mathbf{A} \leftrightarrow \mathbf{B}$ non è che un'abbreviazione per $(\neg \mathbf{A} \vee \mathbf{B}) \wedge (\neg \mathbf{B} \vee \mathbf{A})$): lo stesso possiamo fare per OR, AND e gli altri circuiti logici discussi nel § 2.6. Ma tali automi restano ancora piuttosto banali, poiché il carattere temporale non svolge alcun ruolo. Il valore di uscita si stabilisce istantaneamente e non dipende in alcun modo della storia precedente. Introduciamo perciò un elemento ritardatore L con l'azione seguente:

$$\neg U(0)$$
$$U(t+1) \leftrightarrow E(t) \qquad \text{per } t = 0, 1, 2, \ldots$$

L'elemento L corrisponde all'incirca a una memoria temporale. Con esso si possono assegnare automi già piú interessanti. Cosí l'automa della figura 10 fornisce l'addizione di due numeri in scrittura binaria, se questi numeri (come in una macchina in serie) sono rappresentati da impulsi elettrici che si susseguono come appare dalla figura 10. S_2 somma mod 2; S_1 calcola il riporto (e si comporta come l'usuale congiunzione) che viene restituito a S_2 attraverso L:

$$U(t) \leftrightarrow (E_1(t) \,\&\, E_2(t) \,\&\, R(t)) \vee (E_1(t) \,\&\, \neg E_2(t) \,\&\, \neg R(t))$$
$$\vee (\neg E_1(t) \,\&\, E_2(t) \,\&\, \neg R(t)) \vee (\neg E_1(t) \,\&\, \neg E_2(t) \,\&\, R(t))$$
$$R(0)$$
$$R(t) \leftrightarrow (E_1(t-1) \,\&\, E_2(t-1)) \vee (E_1(t-1) \,\&\, \neg E_2(t-1) \,\&\, R(t-1))$$
$$\vee (\neg E_1(t-1) \,\&\, E_2(t-1) \,\&\, R(t-1)).$$

Nel sistema interviene il predicato ausiliare R, che sta a significare la presenza del riporto. Inoltre, la caratterizzazione di U è per induzione e non-esplicita. Si ottiene però una caratterizzazione esplicita di U in dipendenza da E_1 e da E_2 scrivendo, nel calcolo dei predicati a un posto del secondo ordine,

$$U(t) \leftrightarrow \exists R(\Phi(E_1, E_2, R, t) \,\&\, \neg R(0) \,\&\, \forall z(z \leq t \rightarrow \Psi(E_1, E_2, R, z)))$$

ove $\Phi(E_1, E_2, R, t)$ e $\Psi(E_1, E_2, R, z)$ sono il secondo membro rispettivamente della prima e della seconda equivalenza scritte sopra. Abbiamo quindi descritto il comportamento dell'automa della figura 10 mediante una formula $\Gamma(E_1, E_2, t)$ della logica dei predicati del secondo ordine a un posto (ove cioè possiamo esprimere locuzioni come 'esiste una proprietà R...'), che definisce il predicato di uscita U corrispondente ai predicati di entrata E_1, E_2 secondo la $U(t) \leftrightarrow \Gamma(E_1, E_2, t)$. Il calcolo delle proposizioni (o dei circuiti, che da esso differisce solo nella terminologia) è dunque insufficiente per automi come questi: un nuovo calcolo formulato in un linguaggio piú espressivo permette invece una descrizione di tali automi. Una trattazione già notevolmente sofisticata a livello di linguaggio «perfetto» permette quindi la «riproduzione» di una

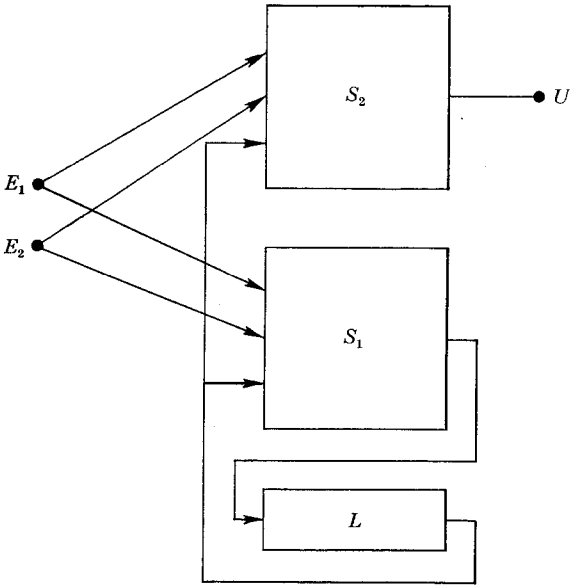


Figura 10.
Circuito di addizione binario.

pratica – il comportamento di macchine calcolatrici intese come automi finiti nel senso di Church – e ripropone a livello piú complesso le questioni di ottimizzazione cui abbiamo accennato per i circuiti logici combinatori nel § 2.6; nel § 5.2 tracceremo un confronto tra le macchine calcolatrici, intese come automi finiti, e la loro idealizzazione, cioè la macchina di Turing intesa come automa crescente.

3. *Il calcolo coi numeri reali e coi numeri complessi.*

3.1. Il calcolo coi razionali come calcolo di coppie.

Riprendiamo in esame i vari sistemi di numeri e i relativi calcoli cui si è accennato nel § 2.3. Il calcolo coi numeri relativi può essere presentato come un calcolo di coppie ordinate di numeri naturali, soggetto a speciali regole operative; è infatti sufficiente introdurre le seguenti definizioni dell'uguaglianza, della somma e del prodotto fra tali coppie, definizioni che possono venire riguardate come ulteriori regole di deduzione in un calcolo dei naturali (cfr. § 2.7):

Z.1. $\langle a, b\rangle = \langle c, d\rangle$ se e solo se $a+d=b+c$
Z.2. $\langle a, b\rangle + \langle c, d\rangle = \langle a+c, b+d\rangle$
Z.3. $\langle a, b\rangle \times \langle c, d\rangle = \langle ac+bd, ad+bc\rangle$.

Basta introdurre le abbreviazioni $+a$ e $-a$ rispettivamente per le coppie standard $\langle a, 0\rangle$ e $\langle 0, a\rangle$, cui per Z.1 ogni coppia è riducibile, per ritrovare i numeri con segno. Con Z.2 e Z.3 si ottengono immediatamente le usuali regole operative del calcolo dei relativi: il lettore, per esempio, può agevolmente giustificare anche per questa via la non piú «misteriosa» regola dei segni, e può inoltre controllare facilmente che gli assiomi I.1-I.5 e II.1-II.5 del § 2.4 sono validi; tuttavia non verificando I.6 il sistema dei relativi non è un corpo (come si suol dire, esso forma solo un anello ordinato).

Analogamente possiamo presentare il calcolo coi razionali come un calcolo di coppie ordinate di numeri relativi. Piú precisamente: nella coppia $\langle a, b\rangle$ i simboli a e b denotano ora «numeri» relativi (cioè coppie di naturali) con $b \neq 0$ tali che

Q.1. $\langle a, b\rangle = \langle c, d\rangle$ se e solo se $ad=bc$
Q.2. $\langle a, b\rangle + \langle c, d\rangle = \langle ad+bc, bd\rangle$
Q.3. $\langle a, b\rangle \times \langle c, d\rangle = \langle ac, bd\rangle$.

Anche in questo caso il lettore può ritrovare servendosi di Q.1, Q.2, Q.3 le usuali regole di calcolo delle frazioni (con segno). In particolare la clausola che il secondo numero di una coppia sia sempre diverso da 0 corrisponde all'esclusione della divisione per zero.

In riduzioni di questo tipo sono compresenti un aspetto logico e uno algoritmico: il primo concerne la chiarificazione degli enti su cui e delle regole con cui opera un calcolo, in modo da dissipare incertezze e ambiguità, il secondo fonda invece procedure effettive di calcolo. Esaminiamo in particolare quest'ultimo aspetto.

I numeri relativi e quelli razionali sono rappresentabili in notazione n-aria, per esempio decimale. Ovviamente gli interi relativi non creano difficoltà alcuna. Piú complicata è la faccenda per i razionali. Un razionale – per semplicità prescindiamo dal segno – può venir espresso da una frazione a/b ridotta ai minimi termini, cioè da una coppia $\langle a, b\rangle$ tale che $\text{MCD}(a, b)=1$ (a e b sono detti in tal caso primi fra loro). Un'opportuna procedura, che generalizza adeguatamente quella che abbiamo dato nel § 2.1, permette di associare ad $\langle a, b\rangle$ in modo univoco uno sviluppo n-ario $(q_0, q_1q_2\ldots q_j\ldots)_n$ ove q_0 denota un intero ≥ 0 grande a piacere, mentre per $j>0$ è $0 \leq q_j \leq n-1$, sicché ogni q_j per $j>0$ può scriversi come una cifra del sistema n-ario. Lo sviluppo n-ario di a/b risulta finito se e solo se esiste un intero positivo s tale che b risulta un divisore di n^s e il numero di cifre dopo la virgola è dato appunto dal piú piccolo s che gode di tale proprietà. Ci sono quindi sviluppi n-ari infiniti: tali sviluppi sono periodici, nel senso che per ogni sviluppo esistono due interi $k \geq 1$ e $h>0$

tali che 1) $q_{t+h}=q_t$ per $t \geq k$, e 2) k e h sono i due piú piccoli interi che godono di questa proprietà. $k-1$ dà il numero delle cifre dell'antiperiodo, h quello delle cifre del periodo. Se $k=1$, lo sviluppo n-ario di $\langle a, b\rangle$ è detto periodico puro (mancando l'antiperiodo). Per convenzione si scrive

$$\langle a, b\rangle = (q_0, q_1\ldots q_{k-1}\overline{q_k\ldots q_{k+h-1}})_n.$$

Il numero razionale $\langle a, b\rangle$ possiede sviluppo periodico puro se e solo se b e n sono primi fra loro. Nel caso generale si può scomporre b in un prodotto b_1b_2 ove b_1 è un divisore di n^s con s intero positivo e b_2 è primo con n. Definito c_1 dalla relazione $b_1c_1=n^s$ risulta $\langle a, b\rangle = \langle 1, n^s\rangle \langle ac_1, b_2\rangle$ ove ac_1 e b_2 sono primi tra loro. $\langle ac_1, b_2\rangle$ possiede quindi lo sviluppo n-ario periodico puro $(q_0, \overline{q_1q_2\ldots q_h})_n$ e pertanto $\langle a, b\rangle$ a causa della divisione per n^s possiede uno sviluppo in cui prima di q_1 ci sono ancora s cifre.

Possiamo dunque limitarci al caso di b primo con n. Si dimostra allora che h è il minimo intero positivo λ per cui b è un divisore di $n^\lambda - 1$ e quindi h non dipende dal numeratore a della frazione. Questo teorema può venir espresso in modo elegante nel linguaggio gaussiano delle congruenze (cfr. § 2.4): h è il piú piccolo λ per cui $n^\lambda \equiv 1 \bmod b$.

Introduciamo ora la cosiddetta funzione φ di Eulero che a ogni intero positivo c fa corrispondere il numero $\varphi(c)$ di tutti gli interi positivi minori di c e primi con c (è, per esempio, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, ecc. e per convenzione $\varphi(1)=1$): è dovuto sostanzialmente a Fermat e a Eulero il fondamentale teorema per il quale $n^{\varphi(b)} \equiv 1 \bmod b$, onde $h \leq \varphi(b)$. (Un risultato ulteriore assicura che h è addirittura un divisore di $\varphi(b)$). Poiché determinare esattamente h per n e b abbastanza grandi può risultare laborioso, la maggiorazione $h \leq \varphi(b)$ appare interessante in quanto da $b=p_1^{m_1}\ldots p_r^{m_r}$ con $p_1, \ldots, p_r$ primi distinti (cfr. il teorema di Gauss ricordato nel § 2.4) si ricava (teorema di Eulero) $\varphi(b)=b\,[1-(1/p_1)]\ldots[1-(1/p_r)]$.

Come è noto, la φ di Eulero svolge un ruolo essenziale in molti settori della teoria dei numeri.

Inversamente ci chiediamo se a una qualsiasi rappresentazione n-aria periodica (pura o mista) corrisponda esattamente una frazione – una coppia – che ha quello sviluppo. La risposta è (in entrambi i casi) affermativa, con esclusione degli sviluppi della forma $(q_0, q_1\ldots q_{k-1}\overline{q_k})_n$ per $q_k=n-1$.

Ciò premesso, osserviamo che sostituire lo sviluppo n-ario – per esempio in base 10 – alle coppie $\langle a, b\rangle$ nel calcolo coi razionali, in forza di una lunga tradizione è certo piú accettato psicologicamente, ma comporta l'inconveniente di aver a che fare con sviluppi infiniti. Anche se a inconvenienti del genere si può ovviare con qualche espediente ad hoc, quale quello di sopralineare le cifre del periodo come abbiamo fatto piú sopra, la rappresentazione dei razionali come coppie ordinate di interi pare piú vantaggiosa. Siccome la rappresentazione su macchina da calcolo può invalidare le regole (proprietà associativa, distributiva, ecc.) piú sopra ricordate e assunte in un approccio formale come assiomi per gli usuali calcoli, nel caso dei razionali l'impiego di coppie ordinate permette almeno in parte di «salvare» tali regole (ovviando agli errori di ar-

rotondamento, ma non a quelli *overflow-underflow*) (per questa terminologia e questa problematica cfr. § 4.3).

3.2. Una procedura per la radice quadrata di un numero razionale.

Riepiloghiamo: un numero finito di operazioni di addizione e di moltiplicazione sui naturali dà come risultato ancora un naturale; diciamo allora che il sistema dei naturali è chiuso rispetto a procedure di calcolo contenenti un numero finito di addizioni e moltiplicazioni. Non è chiuso invece rispetto alle operazioni inverse di sottrazione e divisione (per un numero $\neq 0$). Il sistema degli interi relativi è chiuso rispetto alle procedure contenenti un numero finito di addizioni, moltiplicazioni e sottrazioni, ma non divisioni. Il corpo dei numeri razionali, infine, è chiuso rispetto alle procedure contenenti un numero finito delle quattro operazioni elementari.

Tuttavia, se si considerano le procedure di calcolo contenenti una successione infinita di operazioni elementari, la situazione cambia completamente e si possono avere i fenomeni piú diversi. Eccone un esempio.

Assegnati un intero m e un razionale $x_0 = \langle a_0, b_0 \rangle$ si definisca la procedura

$$\begin{aligned} x_1 &= \langle a_1, b_1 \rangle = \langle a_0^2 + m b_0^2, 2a_0 b_0 \rangle \\ x_2 &= \langle a_2, b_2 \rangle = \langle a_1^2 + m b_1^2, 2a_1 b_1 \rangle \\ &\cdots\cdots\cdots\cdots \\ x_{n+1} &= \langle a_{n+1}, b_{n+1} \rangle = \langle a_n^2 + m b_n^2, 2a_n b_n \rangle \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

Cominciamo con l'osservare che tale procedura *non* è definita se $a_0 = 0$ o se si perviene ad $a_{n+1} = a_n^2 + m b_n^2 = 0$ per qualche n, il che implica $m < 0$. Viceversa, se per qualche n è $m < 0$, si può mostrare che, qualora la procedura non si arresti (e cioè, sia sempre $a_{n+1} \neq 0$), allora i numeri x_n cambiano di segno e diventano arbitrariamente grandi in valore assoluto (il lettore può verificare tale fatto prendendo per esempio $m = -1$ ed $x_0 = \langle 2, 1 \rangle$).

Per $m \geq 0$ invece si ha $x_{n+1} < x_n$ per ogni $n \geq 1$ comunque si sia scelto $x_0 > 0$ come è facile verificare; inoltre lo scarto fra x_n ed x_{n+1} diminuisce sempre almeno per n abbastanza grande giacché per tali n risulta $|x_{n+1} - x_n| \leq |x_n - x_{n-1}|/2$ dove abbiamo usato la notazione come frazione per semplicità.

Illustriamo la procedura su due esempi.

Sia $m = 4$ ed $x_0 = \langle 1, 1 \rangle$; allora

$$\begin{aligned} x_1 &= \langle 5, 2 \rangle = 2{,}5 \\ x_2 &= \langle 41, 20 \rangle = 2{,}05 \\ x_3 &= \langle 3281, 1640 \rangle = 2{,}000609\ldots \\ x_4 &= \langle 21\,523\,361, 10\,761\,680 \rangle = 2{,}000000\ldots \end{aligned}$$

e quindi tale procedura permette di trovare la radice quadrata aritmetica di 4, cioè l'intero positivo x tale che $x^2 = 4$.

Sia ora $m = 2$ ed $x_0 = \langle 1, 1 \rangle$; allora

$$\begin{aligned} x_1 &= \langle 3, 2 \rangle = 1{,}5 \\ x_2 &= \langle 17, 12 \rangle = 1{,}41\bar{6} \\ x_3 &= \langle 577, 408 \rangle = 1{,}414215\ldots \\ x_4 &= \langle 665\,857, 470\,832 \rangle = 1{,}414213\ldots \end{aligned}$$

e inoltre $1{,}5^2 = 2{,}25$; $1{,}416^2 = 2{,}005056$; $1{,}414215^2 = 2{,}000004$; $1{,}414213^2 = 1{,}999998\ldots$

Da questi due esempi il lettore può inferire che la procedura di calcolo ora descritta – che è un caso particolare del metodo di Newton (cfr. § 4.5) – fornisce un'approssimazione di $\sqrt{m}$ per $m \geq 0$. Tuttavia $\sqrt{m}$ può non essere un numero razionale. Per esempio, $\sqrt{2}$ non è un razionale: infatti se fosse $\langle p, q \rangle = \sqrt{2}$ con p e q interi primi fra loro, per definizione di radice quadrata (cfr. § 2.3) si avrebbe $\langle p, q \rangle^2 = 2$ onde $p^2 = 2q^2$, il che è assurdo come il lettore può agevolmente verificare sfruttando la decomposizione in fattori primi. $\sqrt{2}$ è forse il piú celebre esempio di irrazionale quadratico, intendendosi per irrazionale quadratico ogni soluzione di un'equazione $ax^2 + bx + c = 0$ con a, b, c interi e $0 < b^2 - 4ac \neq r^2$ per ogni r intero. Lo studio degli irrazionali quadratici, un ordine di idee promosso da Eulero, Lagrange, Gauss, ecc., ha svolto un ruolo chiave nello sviluppo della teoria dei numeri (vi ritorneremo piú avanti nel § 3.3).

Come abbiamo accennato nel § 2.3, la 'scoperta' degli irrazionali segnò per i Greci una profonda frattura tra aritmetica e geometria, tra matematica del discreto e matematica del continuo. La terminologia stessa è significativa: al greco ἄλογος per 'irrazionale' (cioè 'non esprimibile con un rapporto numerico'), si affiancano termini come ἄρρητος, cioè οὐ ῥητός 'non dicibile', ἄμετρος 'incommensurabile' o addirittura οὐκ ἐν ἀριθμοῖς, cioè 'non numero', «termini non rigorosamente sinonimi» [Michel 1950, p. 414] che insistono rispettivamente sulle difficoltà di espressione (cioè di notazione), sulla dicotomia continuo (geometria) / discreto (aritmetica), sull'esclusione degli irrazionali dai veri e propri numeri.

Punti di vista che riemergono a distanza di secoli: nel caso di un numero che non sia un quadrato perfetto «mai si potrà per pratica alcuna numerare la sua radice aponto assegnare», dice Pacioli, ma «aponto se darano per via de linee e geometria»; il suo contemporaneo Chuquet in *Le triparty en la science des nombres* (1484) dichiara che estrarre radici *imparfaictes* (cioè approssimate) è «fatica senza utilità», anche se aggiungeva che si deve andare avanti «per conseguire la perfezione»; nel Cinquecento Rafael Bombelli osserva ancora che «la Radice quadrata è il lato di un numero non quadrato: il quale è impossibile poterno nominare: però si chiama Radice sorda, overo indiscreta» [1579] cercando nella geometria la via d'uscita all'inadeguatezza del linguaggio aritmetico.

3.3. Continuità e numeri reali.

«Ad ogni modo, nonostante le premesse teoriche e le riserve, Chuquet e Pacioli e Tartaglia e Bombelli, come Greci e Arabi prima di loro, estraevano radici di numeri, quadrati o meno che fossero» [Picutti 1977, p. 160]. La pratica matematica, di fatto, disponeva di un'idea ingenua di numero reale che «si può esprimere dicendo che un numero si considera definito dalla possibilità di ottenere dei valori approssimati e di introdurre questi ultimi nel calcolo. Ciò del resto implica necessariamente un certo grado di confusione fra le misure di grandezza date dall'esperienza, che naturalmente non sono suscettibili di approssimazione indefinita, e dei numeri come $\sqrt{2}$ (ammesso che vi sia un algoritmo per l'approssimazione indefinita di quest'ultimo). Tale punto di vista "pragmatista" riappare quindi in tutte le scuole matematiche nelle quali la maestria del calcolo ha la meglio sugli scrupoli rigoristici e sulle preoccupazioni teoriche» [Bourbaki 1960, trad. it. p. 148].

Uno dei piú grandi successi della matematica greca classica è la teoria eudossiana delle grandezze, magistralmente esposta nel quinto libro degli *Elementi* di Euclide: la retta geometrica – il continuo lineare – diventa il modello privilegiato per l'insieme dei numeri reali e i metodi della geometria forniranno gli standard del rigore matematico fino alla metà del secolo scorso. Ma, come abbiamo visto, l'algebra nel Cinquecento e l'analisi nel Seicento e nel Settecento si svilupparono però in aperta violazione di questi canoni, recuperati, anche se in un quadro concettuale diverso, da Gauss e da Cauchy, solo agli inizi dell'Ottocento.

Cosí Cauchy, per esempio, nell'introduzione al celebre *Cours d'Analyse* [1821] contrappone rigore geometrico e pratica algebrica: «Per quanto riguarda i metodi, ho cercato di dare loro tutto il rigore richiesto nella geometria in modo da non ricorrere mai ai ragionamenti tratti dalla genericità dell'algebra. Ragionamenti di tale fatta, benché siano usualmente accettati, in particolare nel passaggio dalle serie convergenti a quelle divergenti e dalle quantità reali alle espressioni immaginarie, non possono a mio avviso essere considerati altro che delle induzioni atte a far intuire talvolta la verità, ma che poco si accordano con la tanto vantata esattezza delle scienze matematiche. Si deve anzi osservare che tali ragionamenti tendono ad attribuire alle formule algebriche un'estensione indefinita, mentre di fatto per la maggior parte tali formule sussistono unicamente sotto opportune condizioni e per opportuni valori delle quantità che esse contengono. Determinando tali condizioni e tali valori, e fissando in modo preciso il significato delle notazioni di cui mi servo, faccio scomparire ogni incertezza; le diverse formule presentano allora solo relazioni tra quantità reali, relazioni che è sempre facile verificare sostituendo numeri alle quantità stesse» [Cauchy 1821, pp. II-IV].

La separazione dell'idea di numero reale dalla teoria delle grandezze e quindi la costruzione di numeri reali a partire dai soli numeri razionali viene ottenuta però solo nella seconda metà dell'Ottocento a opera di Weierstrass, Dedekind, Méray e Cantor che completano la rigorizzazione di Cauchy. L'impiego del metodo assiomatico infine fa slittare il problema dell'esistenza dei numeri reali in quello della non-contraddizione degli assiomi che implicitamente li definiscono, questione spesso riportata nel contesto piú ampio della teoria degli insiemi (si veda per la teoria assiomatica degli insiemi e la connessa questione di non-contraddittorietà l'articolo «Assioma/postulato» di questa stessa *Enciclopedia*).

Per definire i numeri reali ci si può limitare quindi ad aggiungere un opportuno assioma della continuità agli assiomi di corpo ordinato dati nel § 2.4.

Premettiamo alcune definizioni. Sia F un corpo (commutativo) ordinato e sia A un sottoinsieme non vuoto di F; diciamo allora che b, elemento di F, è un maggiorante di A quando $a \leq b$ per ogni a di A; se A ammette un maggiorante, allora A è detto limitato superiormente; b è detto estremo superiore di A, e si scrive $b = \sup A$ quando b è un maggiorante di A e ogni $c < b$ non è maggiorante di A; se poi b appartiene ad A diciamo che è il massimo di A. Ciò premesso, l'insieme $\mathbf{R}$ dei numeri reali è un corpo commutativo (cfr. p. 393) ordinato (cfr. p. 396) che verifica il seguente assioma:

III. *Se $A \subseteq \mathbf{R}$ è un insieme non vuoto e limitato superiormente, allora A ammette estremo superiore.*

Possiamo definire in modo analogo i concetti di minorante, limitato inferiormente, estremo inferiore ($b = \inf A$) e minimo ed avere una proposizione equivalente a III. Piú profondo è osservare che l'assioma III è equivalente all'asisoma (detto di Dedekind):

III′. *Siano A e B sottoinsiemi di $\mathbf{R}$ tali che:*

I) $A \cup B = \mathbf{R}$

II) $A \neq \emptyset$ e $B \neq \emptyset$

III) *Se $a \in A$ e $b \in B$ allora $a < b$.*

Esiste allora un α in $\mathbf{R}$ tale che $\alpha < x$ implica $x \in B$ e $x < \alpha$ implica $x \in A$.

Da III (o da III′) si deduce facilmente il cosiddetto principio di Archimede:

IV. *Per ogni x positivo e per ogni y esiste un intero ≥ 0 tale che $nx > y$.*

Un'immediata conseguenza è che dati due reali a, b con $a < b$, esiste un numero razionale r compreso tra a e b. Questo risultato ci permette di approssimare i reali con i razionali e costituisce il fondamento teorico della pratica abituale della misurazione (si veda l'articolo «Approssimazione» di questa stessa *Enciclopedia*, al § 1).

Ricordiamo che una successione (a_n) di numeri reali è un'applicazione dell'insieme dei naturali $\mathbf{N}$ in $\mathbf{R}$; una successione (a_n) di reali è detta poi convergente al limite λ se per ogni $\varepsilon > 0$ esiste un $n_0 \in \mathbf{N}$ tale che $n > n_0$ implica $|a_n - \lambda| < \varepsilon$; è detta successione di Cauchy se per ogni $\varepsilon > 0$ esiste un $n_0 \in \mathbf{N}$ tale che $n, m > n_0$ implica $|a_n - a_m| < \varepsilon$. È facile verificare che una successione

convergente è di Cauchy. Un'implicita conseguenza di III è la proprietà inversa, nota anche come criterio di convergenza di Cauchy:

V. (Proprietà di completezza). *Ogni successione di Cauchy è convergente.*

Di tale proprietà non godono per esempio i numeri razionali (come si evince dall'esempio del § 3.2); in effetti le proprietà IV e V possono essere assunte come assiomi della continuità. Osserviamo tuttavia che IV in tale contesto è essenziale: esistono infatti campi ordinati (e completi nel senso di V) che non soddisfano IV: un celebre esempio è dovuto a Veronese. L'idea di corpo ordinato non-archimedeo è del resto alla base delle ricerche di analisi non-standard promosse da Robinson e Luxemburg negli anni '60.

La definizione di limite di una successione sopra introdotta permette di giustificare, nell'ambito dei numeri reali, l'utilizzazione di somme, prodotti e quozienti con infiniti termini; illustriamo rapidamente tali concetti che si sono rivelati fra i piú fecondi dell'analisi.

Alla successione di numeri reali (a_n) associamo la successione

$$\begin{aligned} s_0 &= a_0 \\ s_1 &= a_0 + a_1 = s_0 + a_1 \\ s_2 &= a_0 + a_1 + a_2 = s_1 + a_2 \\ &\cdots\cdots\cdots \\ s_n &= a_0 + a_1 + \ldots + a_n = s_{n-1} + a_n \\ &\cdots\cdots\cdots \end{aligned}$$

Se la successione s_n è convergente al limite s si dice che s è la somma della serie di termine generale a_n e si scrive per convenzione

$$s = \sum_{n=0}^{\infty} a_n .$$

La serie è invece detta divergente se la successione (s_n) è divergente, cioè se per ogni $\varepsilon > 0$ esiste n_0 tale che $n \geq n_0$ implica $|s_n| > \varepsilon$.

In modo analogo se la successione

$$\begin{aligned} p_0 &= a_0 \\ p_1 &= a_0 a_1 = p_0 a_1 \\ p_2 &= a_0 a_1 a_2 = p_1 a_2 \\ &\cdots\cdots\cdots \\ p_n &= a_0 a_1 \ldots a_n = p_{n-1} a_n \\ &\cdots\cdots\cdots \end{aligned}$$

è convergente al limite p si dice che p è il valore del prodotto infinito di termine generale a_n e si scrive per convenzione

$$p = \prod_{n=0}^{\infty} a_n .$$

Se inoltre la successione

$$\begin{aligned} q_0 &= a_0 \\ q_1 &= a_0 + 1/a_1 \\ q_2 &= a_0 + 1/(a_1 + 1/a_2) \\ &\cdots\cdots\cdots \\ q_n &= a_0 + 1/(a_1 + 1/(a_2 + \ldots + 1/(a_n)\ldots)) \\ &\cdots\cdots\cdots \end{aligned}$$

è convergente al limite q si dice che q è il valore della frazione continua infinita e si scrive per convenzione $a = /a_0, a_1, \ldots, a_n, \ldots/$.

Tenendo conto di tali definizioni il lettore può agevolmente adattare il criterio di convergenza di Cauchy per le successioni al caso delle serie, dei prodotti infiniti e delle frazioni continue infinite.

Fra le molteplici applicazioni delle serie vogliamo ricordare il modo con il quale si ottiene la rappresentazione n-aria di un numero reale x completando cosí quanto si è detto per la rappresentazione n-aria di naturali, interi e razionali (cfr. §§ 2.1 e 3.1). Per semplicità assumiamo x positivo e minore di 1. Per il principio di Archimede esiste un intero q_1 con $0 \leq q_1 \leq n-1$ tale che $q_1/n \leq x < (q_1+1)/n$, se poi $x - (q_1/n) > 0$ allora esiste un intero q_2 con $0 \leq q_2 \leq n-1$ tale che $q_2/n^2 \leq x - (q_1/n) < (q_2+1)/n^2$; proseguendo in questo modo si costruisce una successione di numeri interi $(q_1, q_2, \ldots, q_k, \ldots)$ ed è possibile provare che

$$x = \sum_{k=1}^{\infty} \frac{q_k}{n^k} .$$

Diremo allora che $(0, q_1 q_2 \ldots q_k \ldots)_n$ è la rappresentazione n-aria di x.

Analogamente al caso dei numeri razionali, a ogni successione $(q_1, q_2, \ldots, q_k, \ldots)$ di interi con $0 \leq q_k \leq n-1$ è infine possibile associare esattamente un numero reale

$$x = \sum_{k=1}^{\infty} \frac{q_k}{n^k}$$

con esclusione delle successioni ove $q_k = n-1$ per $k \geq k_0$.

Peraltro i numeri reali possono essere anche rappresentati mediante le frazioni continue *regolari*, mediante cioè quelle frazioni continue per cui a_k è un numero intero positivo per ogni $k \geq 1$. Nel caso particolare in cui x sia un irrazionale quadratico allora la frazione continua regolare è anche periodica. (Questo teorema, dovuto a Lagrange, fornisce l'analogo della rappresentazione decimale periodica dei razionali esposta nel § 3.1).

La presentazione dei reali qui abbozzata (in particolare la proprietà V) mette in luce il ruolo che svolge già a questo livello il concetto di limite, idea su cui si fonda gran parte dell'edificio dell'analisi. Sarà facile al lettore ripercorrere tale cammino estendendo in modo naturale a funzioni di **R** in **R** le definizioni date sopra per successioni (cioè applicazioni di **N** in **R**) di limite finito ($f(x)$ tende a λ per x che tende a x_0 quando per ogni $\varepsilon > 0$ esiste $\delta > 0$ tale che $0 < |x - x_0| < \delta$ implica $|f(x) - \lambda| < \varepsilon$, in simboli $\lim_{x \to x_0} f(x) = \lambda$; si veda del resto

l'articolo «Applicazioni» di questa stessa *Enciclopedia* al § 3.4) e di limite infinito. La funzione $f(x)$ si dirà poi continua in x_0 se $\lim_{x\to x_0} f(x)=f(x_0)$. Per i limiti di funzioni (o di successioni) si stabilisce immediatamente un calcolo formale ($\lim(f+g)=\lim f+\lim g$, $\lim(f\cdot g)=\lim f\cdot \lim g$, ecc.), che permette fra l'altro di verificare che le funzioni continue formano uno spazio vettoriale, addirittura un'algebra su **R** (per queste nozioni, si veda ancora l'articolo «Applicazioni», § 3.2).

Ricordiamo anche alcune proprietà globali delle funzioni continue:

a) sia f una funzione definita continua nell'intervallo chiuso e limitato $[a, b]$, allora l'insieme dei valori assunti da f in $[a, b]$ ammette massimo e minimo (teorema di Bolzano-Weierstrass);
b) una funzione continua trasforma intervalli in intervalli;
c) se f è continua e strettamente crescente (cioè se $x_1<x_2$ implica $f(x_1)<f(x_2)$), allora la funzione inversa è continua e strettamente crescente.

Per esempio la funzione $x\to x^n$ è continua e strettamente crescente per $x\geq 0$ qualunque sia n intero ≥ 2. Esiste dunque la sua funzione inversa (continua, strettamente crescente e definita per $x\geq 0$) detta radice n-esima aritmetica.

L'algebra dei limiti, non appena teniamo conto anche del limite infinito, porta naturalmente a completare il continuo lineare con un punto all'infinito che denoteremo al solito con il simbolo ∞. In tale modo la retta risulta omeomorfa (cfr. l'articolo «Applicazioni», § 3.5) alla circonferenza (compattificazione di Hausdorff). Si badi però che la relazione di ordine $\leq$ non si estende in modo naturale da **R** a $\mathbf{R}\cup\{\infty\}$.

In effetti, matematici come John Wallis ed Eulero vedevano nei numeri negativi numeri «plus quam infiniti», ragionando nel modo seguente. I numeri $1/3$, $1/2$, $1/1$, $1/0$ formano una successione crescente, in termini generici $1/m<1/(m-1)$. Per $m=0$ si ricava $1/0<1/(-1)$ cioè $\infty<-1$. In realtà tale idea appare del tutto plausibile: usualmente manteniamo valida la formula $m>m-1$ per $m=0$ e in tal caso sacrifichiamo la formula $1/m<1/(m-1)$, ma nulla ci vieta, appunto, di fare l'inverso, sostituendo, per cosí dire, alla retta dei numeri il cerchio dei numeri.

Possiamo aggirare difficoltà del genere completando in modo diverso il continuo lineare. Aggiungiamo formalmente i simboli $-\infty$, $+\infty$ con le regole algebriche: $a\pm\infty=\pm\infty$, $(+\infty)+(+\infty)=+\infty$, $(-\infty)+(-\infty)=-\infty$, $a\cdot(\pm\infty)=\pm\infty$ per $a>0$, $a\cdot(\pm\infty)=\mp\infty$ per $a<0$, $(\pm\infty)(\pm\infty)=\pm\infty$ secondo la regola dei segni; e con l'ordine $-\infty<x<+\infty$ per ogni x di **R**. La retta numerica cosí completata, $\mathbf{R}\cup\{-\infty, +\infty\}$ risulta omeomorfa a un intervallo chiuso di **R**: basta considerare, per esempio, la funzione $f(x)=x/(1-|x|)$ definita per $-1<x<+1$ e osservare inoltre che $\lim_{x\to -1} f(x)=-\infty$ e $\lim_{x\to +1} f(x)=+\infty$ (ove è stata estesa in modo naturale la definizione di limite infinito: per esempio, $\lim_{x\to x_0} f(x)=+\infty$ significa che per ogni $\varepsilon>0$ esiste $\delta>0$ tale che $0<|x-x_0|<\delta$ implica $f(x)>\varepsilon$).

3.4. Maggiorare/minorare/approssimare.

«Per acquisire il "senso dell'analisi" indispensabile fin nelle speculazioni piú astratte bisogna aver imparato a distinguere ciò che è "grande" da ciò che è "piccolo", ciò che è "dominante" e ciò che è "trascurabile". In altri termini il calcolo infinitesimale... consiste nell'imparare a maneggiare delle *disuguaglianze* piuttosto che delle uguaglianze e si potrebbe riassumere in tre parole: MAGGIORARE, MINORARE, APPROSSIMARE» [Dieudonné 1968, p. 9].

È proprio in tale ottica che si utilizzano i procedimenti calcolistici basati sul concetto di limite e le sue applicazioni alle serie, prodotti infiniti e frazioni continue.

L'uso spregiudicato di tali procedimenti ha permesso a grandi matematici del Settecento, come Eulero, di conseguire risultati notevoli; alcuni di questi vennero riottenuti dai matematici della prima metà dell'Ottocento nel contesto di una discussione della nozione di convergenza condotta «in modo estremamente rigoroso, e fatta per soddisfare coloro le cui preferenze vanno ai metodi rigorosi dei geometri antichi» [Gauss 1813, ed. 1866 III, p. 139].

Ma il punto di vista è radicalmente cambiato. Eulero [1755, §§ 108-11]: «Diciamo dunque che la somma di una serie infinita è l'espressione finita, dal cui sviluppo viene generata la serie stessa. In tal senso la somma della serie infinita $1-x+x^2-x^3+\ldots$ sarà $1/(1+x)$ poiché la serie si ottiene dallo sviluppo della frazione, qualunque numero si metta al posto di x. Se ci accordiamo su questo, la nuova definizione della parola somma coincide con il significato usuale quando la serie converge; e poiché le serie divergenti non hanno somma in senso proprio del termine, nessun inconveniente può sorgere dalla nostra terminologia». Cauchy [1821, p. IV], quasi rispondesse direttamente ad Eulero: «È duro [ammettere] di primo acchito [che] una serie divergente non ha somma», ma è rinunzia necessaria se si vuol restare «fedeli» ai principî del rigore. Un punto di vista destinato a durare per buona parte dell'Ottocento almeno sino ai risultati ottenuti da Poincaré e alla trattazione rigorosa degli sviluppi asintotici di Landau e di Hardy, variamente motivata (dalla meccanica celeste al teorema dei numeri primi). Il punto di vista formale adombrato nel passo di Eulero è recuperato invece nell'ambito delle serie formali di potenze che svolgono oggi un ruolo importante in varie direzioni.

Maggiorare, minorare e approssimare i numeri reali è facile sfruttando la rappresentazione n-aria (cfr. § 3.3), basata sull'utilizzazione di una unità di misura e sul principio di Archimede.

Assai piú complicata è la situazione quando si confrontino funzioni infinitesime (rispettivamente infinite) in un intorno del punto x_0; ricordiamo che la funzione $f(x)$ è detta infinitesima per x tendente ad x_0 se $\lim_{x\to x_0} f(x)=0$, infinita per x tendente ad x_0 se $\lim_{x\to x_0} |f(x)|=\infty$. Tuttavia il comportamento delle funzioni, poniamo, infinite per x tendente ad x_0 può essere assai diverso, come risulta dalla tabella 1.

Tabella 1.

Valori assunti da alcune funzioni per x vicino ad $x_0 = +\infty$. (I numeri in corsivo sono da prendersi come ordine di grandezza; $10^{3\cdot 10^{29}}$ significa $10^{300\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000}$).

	$\log x$	x	x^2	2^x	2^{2^x}
1	1	1	1	2	4
2	0,693	2	4	4	16
5	1,609	5	25	32	$4{,}3\cdot 10^9$
10	2,303	10	10^2	1024	$1{,}8\cdot 10^{308}$
10^2	4,605	10^2	10^4	10^{30}	$10^{3\cdot 10^{29}}$
10^3	6,908	10^3	10^6	10^{301}	$10^{3\cdot 10^{300}}$
10^4	9,110	10^4	10^8	10^{3010}	$10^{3\cdot 10^{3009}}$
10^5	11,510	10^5	10^{10}	10^{30103}	$10^{3\cdot 10^{30102}}$

Analoghi esempi si possono dare per funzioni infinitesime. Osserviamo poi che usando il cambiamento di coordinate $x' = 1/(x - x_0)$ ci si può limitare a confrontare le funzioni infinite ed infinitesime in un intorno di $+\infty$ ovvero di 0. Per semplicità ci limiteremo a confrontare le funzioni infinite per x tendente a $+\infty$.

Siano f e g due tali funzioni e consideriamo il loro quoziente $h = f/g$; distinguiamo i seguenti quattro casi per x tendente a $+\infty$:

I) h è infinitesimo ed allora si dice che g è un infinito di ordine superiore ad f;
II) h è infinito ed allora si dice che f è un infinito di ordine superiore ad f;
III) esistono costanti $0 < a < A < +\infty$ (ovvero $-\infty < B < b < 0$) per cui risulta sempre $a \leq h(x) \leq A$ (oppure sempre $B \leq h(x) \leq b$) ed allora si dice che f e g sono infinite dello stesso ordine;
IV) altrimenti, f e g non sono confrontabili.

Si dice inoltre piú precisamente che f è asintotico a g (per x tendente a $+\infty$) quando risulta $\lim_{x\to+\infty} h(x) = 1$ (ed allora si è necessariamente nel caso III); si usa in tal caso la notazione $f \sim g$.

Un esempio per IV si ha prendendo (per x grande) $f(x) = x \sin^2 x + x^2 \cos^2 x$ e $g(x) = x^2 \sin^2 x + x \cos^2 x$.

Ricordiamo inoltre che si scrive $f = O(g)$ quando $|f(x)/g(x)|$ è limitato superiormente in un intorno di $+\infty$.

Limitiamoci naturalmente a considerare infiniti confrontabili in un intorno di $+\infty$; preso un infinito campione $g(x)$ diremo che $f(x)$ ha ordine k (reale >0) rispetto a $g(x)$ se $f(x)$ risulta dello stesso ordine di $g^k(x)$. È facile verificare che $\log |g(x)|$ è allora un infinito di ordine inferiore a tutte le potenze reali positive di $g(x)$ mentre $e^{|g(x)|}$ è un infinito di ordine superiore a tutte le potenze di $g(x)$. Vediamo cosí che l'usuale scala numerica non è adeguata; il principio di Archimede non vale anche limitandosi a infiniti confrontabili.

Ritornando al problema delle serie divergenti, si sceglie come funzione campione $g(x)$ una funzione il cui comportamento (per x tendente a $+\infty$) si ritiene sufficientemente noto (per esempio $g(x) = x$) e si classificano le serie divergenti in base al confronto con tale campione. È questo il nucleo della moderna teoria degli sviluppi asintotici che si è rivelata particolarmente fruttuosa nella teoria analitica dei numeri; per esempio il celebre teorema dei numeri primi di Hadamard e di La Vallée - Poussin asserisce che il numero $\pi(x)$ dei primi minori di x è asintotico a $x/\log x$ e tende ad essere un po' piú grande di tale valore, come risulta anche dalla seguente tabella:

x	$\pi(x)$	$x/\log x$
10^3	168	145
10^6	78 498	72 382
10^9	50 847 534	48 254 942

La famosa ipotesi di Riemann, tuttora non dimostrata, precisa il comportamento di $\pi(x)$ per x tendente a $+\infty$ colla formula:

$$\pi(x) = \int_2^x \frac{1}{\log t}\, dt + R(x)$$

ove, per ogni $\varepsilon > 0$, $|R(x)| = O(x^{1/2+\varepsilon})$; ricordiamo che $\int_x^2 (1/\log t)\, dt$ è asintotico proprio a $x/\log x$.

Vogliamo ricordare ancora l'applicazione fatta da Eulero degli sviluppi asintotici alla valutazione della serie armonica

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} = \log n + \gamma + \frac{1}{2n} + \gamma_n$$

ove il resto γ_n è infinitesimo di ordine superiore a $1/n$ per n tendente a $+\infty$ e γ è la costante di Eulero un cui valore approssimato è $\gamma^* = 0{,}57721$.

Valutare quanto $\gamma^* = 0{,}57721$ approssimi la costante di Eulero γ è un esempio della problematica connessa alla nozione generale di approssimazione. Carnot, nelle sue *Réflexions sur la métaphysique du calcul infinitésimal* coglie il nocciolo della questione: «Quando è troppo difficile trovare la soluzione esatta di un problema, è naturale tentare almeno di approssimarla il piú possibile, trascurando le quantità che imbarazzano le combinazioni [*combinaisons*], purché si preveda che tali quantità trascurate non possono, dato il loro piccolo valore, produrre altro che un errore del pari trascurabile nel risultato del calcolo» [1797, ed. 1921 p. 4].

È, sostanzialmente, un problema di *credibility gap* 'intervallo di confidenza': non si sa quanto credere nell'approssimazione trovata. Fin dal Seicento i matematici hanno incontrato tale problematica nella costruzione delle tavole dei logaritmi (e piú tardi di altre funzioni speciali). In effetti, come si è visto nel § 3.3, i numeri reali hanno una rappresentazione decimale (in generale non-periodica) con infinite cifre; simboli ad hoc furono introdotti per speciali numeri reali: π (lunghezza della circonferenza di diametro 1), e (base dei logaritmi

naturali), γ (la costante di Eulero sopra ricordata), ecc., ma ciò non risolve ovviamente il problema generale: nella pratica si impiegano rappresentazioni decimali con un numero finito di cifre e si commette cosí un errore di approssimazione.

Nella pratica scientifica occorre tener presenti ovviamente altri tipi di errore quali gli errori connessi con la rilevazione dei dati sperimentali. Questo nostro accenno alla dicotomia esatto/approssimato rimanda naturalmente a una teoria sistematica degli errori che storicamente si è cominciata a delineare all'inizio dell'Ottocento con Gauss e Laplace. Di fronte al problema del *credibility gap* si deve innanzitutto supporre che esista il valore esatto e questo primo assunto è ragionevole proprio alla luce della teoria dei numeri reali data nel § 3.1. Si tratta poi di stabilire un criterio che permetta di costruire, partendo dalle approssimazioni trovate, il «valore piú probabile» del valore esatto di cui ovviamente il ricercatore ha solo un'idea congetturale.

Un primo punto di vista (Gauss in *Teoria motus corporum coelestium*, 1809) consiste nel fissare in prima ipotesi la scelta del valore piú probabile e ricavare conseguentemente la distribuzione dell'errore.

Un secondo punto di vista (Laplace e piú tardi Bessel) consiste nel fissare invece la distribuzione di probabilità dell'errore e nel ricavarne quindi la stima del valore piú probabile del valore vero.

Concludiamo osservando che in tale contesto Laplace ottiene per integrazione per parti il seguente sviluppo asintotico della funzione di errore:

$$\operatorname{Erfc}(x) = \int_x^{+\infty} e^{-t^2}\,dt \sim \frac{e^{-x^2}}{2x} \sum_{m=0}^{\infty} \frac{(-1)^m (2m)!}{m!\,(2x)^{2m}}.$$

La serie in questione è divergente ma Laplace ha usato tale serie per calcolare $\operatorname{Erfc}(x)$ per valori grandi di x. Sempre in tale contesto Laplace ha studiato il comportamento asintotico per $t \to +\infty$ di integrali del tipo

$$I(t) = \int_0^{+\infty} g(x)\, e^{t\,h(x)}\,dx.$$

3.5. Derivazione e integrazione.

Utilizzando il concetto di limite s'introduce la nozione di funzione differenziabile nel punto x_0 e di derivata di f nel punto x_0. Precisamente, sia $f(x)$ una funzione definita in un intorno del punto x_0; si dice che f è derivabile (o differenziabile) nel punto x_0 se esiste un numero reale A tale che

$$(1) \qquad f(x_0+h) = f(x_0) + Ah + h\,\varepsilon(h)$$

ove $\varepsilon(h)$ è una funzione infinitesima per h tendente a 0. A è detto derivata di f in x_0 (e indicato con uno dei simboli $f'(x_0)$, $\dot{f}(x_0)$, $Df(x_0)$, $(df/dx)(x_0)$, ...). Se f è derivabile in ogni punto dell'intervallo I si può definire in I la (funzione) derivata di f (e indicata con f', $\dot{f}$, Df, ...).

Come è noto la derivata ammette un'interpretazione geometrica (coefficiente angolare della tangente al grafico di f nel punto $(x_0, f(x_0))$ ed una cinematica (velocità o flussione), ma qui privilegiamo, nell'ottica maggiorare/minorare/approssimare, l'aspetto di approssimazione che tra l'altro permette di estendere tale definizione al caso generale di una applicazione da $\mathbf{R}^n$ in $\mathbf{R}^m$ come osservato nell'articolo «Applicazioni» di questa stessa *Enciclopedia* (I, p. 724).

La continuità di f in x_0 è condizione necessaria, ma non sufficiente, per la derivabilità; mentre quindi per ogni funzione costruita esplicitamente (con procedura finita) da funzioni elementari è possibile determinarne esplicitamente la derivata prima, e quindi iterare quanto si vuole il procedimento (derivate successive), in generale per una funzione continua ciò non si dà. Questo ostacolo è brillantemente superato con la teoria delle distribuzioni. (Come osserva Schwartz [1966, pp. 84-85], «abbiamo introdotto le distribuzioni per poter derivare le funzioni continue: vediamo che non abbiamo introdotto nulla di troppo, poiché [si dimostra che], dal punto di vista locale, ogni distribuzione è la derivata di una funzione continua»).

Data la funzione $f(x)$ definita in un intervallo I, diremo poi che la funzione $F(x)$ è una primitiva (o un integrale) di $f(x)$ in I quando $DF(x) = f(x)$ per ogni x di I. Scriveremo, al solito, $F(x) = \int f(x)\,dx$. Analogamente al calcolo algebrico (addizione/sottrazione, moltiplicazione/divisione) il calcolo della primitiva appare come operazione inversa della derivazione; ma la determinazione della primitiva non è univoca ($F(x)$ integrale di $f(x)$ in I è infatti determinata a meno di una costante additiva arbitraria). Inoltre la determinazione di una primitiva di una funzione $f(x)$ costruita esplicitamente (con procedura finita) da funzioni elementari è questione delicata. Già una primitiva di $1/x$ è la funzione $\log x$, una primitiva di $1/(1+x^2)$ è $\operatorname{arctg} x$, ecc.: da funzioni razionali si perviene quindi a funzioni «speciali»; piú in generale integrali come $\int f(x, e^x)\,dx$, $\int f(x, \cos x, \sin x)\,dx$, ecc. ove f è algebrico o addirittura razionale, dànno luogo a nuove funzioni «speciali» (teorema di Liouville), alcune delle quali hanno avuto un grande ruolo nell'analisi (per esempio i cosiddetti integrali ellittici).

Questo modo d'introdurre «nuove funzioni», diventato pressoché canonico ancora nella fase pionieristica del calcolo infinitesimale (diciamo con Eulero), viene meno con l'indagine del concetto di funzione promossa dai matematici della scuola tedesca verso la metà dell'Ottocento: perde interesse, nel contesto di una teoria astratta sufficientemente generale, definire con le primitive nuove famiglie di funzioni, a meno che non siano richieste da particolari esigenze applicative o teoriche. È il paradigma di come muore una tradizione matematica.

Il calcolo integrale sopravvive però nella direzione indicata da un'altra delle sue motivazioni iniziali, quella del calcolo delle aree e dei volumi che rappresenta il naturale sviluppo di problemi già presenti nella matematica greca, per esempio con Archimede.

Per semplicità trattiamo qui solo il problema dell'area delle figure nel piano euclideo in cui supponiamo fissato un riferimento cartesiano ortogonale. Cominciamo col definire l'area (o misura piana) di un rettangolo E come prodotto

della base per l'altezza. Il calcolo dell'area del rettangolo è ricondotto alle misure dei segmenti: in base a quanto visto nel § 3.3 si esprime la lunghezza di un segmento con un numero reale ≥ 0; conseguentemente l'area di E è un numero reale ≥ 0. A partire dall'area del rettangolo si può definire l'area di un triangolo e quindi di ogni poligono come unione di un numero finito di triangoli che sono disgiunti o hanno in comune solo dei lati o parti di lati.

La fase seguente consiste nel definire l'area per figure piú generali quali le regioni con frontiera curva (per esempio area di un cerchio, di un settore di parabola, di iperbole, ecc.). A questo punto il problema presenta due aspetti: 1) definizione di una classe di sottoinsiemi $E \subseteq \mathbf{R}^2$ per i quali l'area è ben definita (insiemi misurabili) e studio delle proprietà generali dell'area; 2) metodo di calcolo di tale area.

Definiamo innanzitutto una famiglia particolare di sottoinsiemi di $\mathbf{R}$ detti figure elementari per le quali la misura dell'area è ben definita. Diremo che due rettangoli chiusi R_1 e R_2 a lati paralleli agli assi sono quasi-disgiunti se tali rettangoli hanno intersezione vuota oppure la loro intersezione si riduce a una parte di un lato; figura elementare un insieme ottenuto come riunione di un numero finito di rettangoli quasi-disgiunti; per comodità diremo che anche l'insieme vuoto $\emptyset$ è una figura elementare. La famiglia di tutte le figure elementari verrà indicata con $\mathfrak{F}\mathfrak{E}$; essa gode delle seguenti proprietà:

E.1. $\emptyset \in \mathfrak{F}\mathfrak{E}$.

E.2. Se $R, S \in \mathfrak{F}\mathfrak{E}$ allora $R \cup S$, $R \cap S$, $R \setminus S$ sono in $\mathfrak{F}\mathfrak{E}$

(per la notazione insiemistica, si veda l'articolo «Assioma/postulato» di questa stessa *Enciclopedia*).

Per induzione si mostra subito che l'unione e l'intersezione di un numero finito di figure elementari è una figura elementare.

Ricordando che l'area del rettangolo chiuso $[a, b] \times [c, d]$ è $(b-a)(d-c)$, l'area della figura elementare viene definita come la somma delle aree dei rettangoli chiusi la cui unione dà E; si verifica senza difficoltà che tale area *non* dipende dalla particolare decomposizione di E in un numero finito di rettangoli a lati paralleli agli assi presa in considerazione. L'area è dunque un'applicazione $\boldsymbol{m} : \mathfrak{F}\mathfrak{E} \to \mathbf{R}$ che gode delle seguenti proprietà:

A.1. $\boldsymbol{m}(E) \geq 0$ per $E \in \mathfrak{F}\mathfrak{E}$.

A.2. $\boldsymbol{m}(\emptyset) = 0$.

A.3. Siano $E, F \in \mathfrak{F}\mathfrak{E}$; se $E \subseteq F$ allora $\boldsymbol{m}(E) \leq m(F)$.

A.4. $\boldsymbol{m}(E \cup F) \leq m(E) + m(F)$ e se $E \cap F = \emptyset$ allora $m(E \cup F) = m(E) + m(F)$.

A.5. Se $E = [a, b] \times [c, d]$ allora $m(E) = (b-a)(d-c)$.

Si osservi che in particolare l'area di un punto o di un segmento è 0 e piú in generale l'area di un numero finito di punti e/o di segmenti è 0.

Vogliamo ora estendere la famiglia degli insiemi misurabili in modo da recuperare in particolare gli insiemi con frontiera curva (del tipo cerchio, settore di parabola, ellisse, iperbole, ecc.).

L'idea intuitiva del metodo consiste nel cercare di approssimare tali insiemi con una successione di figure elementari.

Sia dapprima G un insieme aperto, non-vuoto e limitato e cioè contenuto nel quadrato $Q_h = \{\langle x, y \rangle \mid |x| \leq h \text{ e } |y| \leq h\}$. La misura di G è l'estremo superiore delle aree delle figure elementari F contenute in G; in simboli

$$m(G) = \sup \{m(F) \mid F \subseteq G,\ F \in \mathfrak{F}\mathfrak{E}\}.$$

Siccome $F \subseteq G \subseteq Q_h$ risulta $m(F) \leq 4h^2$ e quindi l'insieme, ovviamente non vuoto, $\{m(F) \mid F \subseteq G,\ F \in \mathfrak{F}\mathfrak{E}\}$ è limitato superiormente; dall'assioma III di $\mathbf{R}$ si deduce che $\boldsymbol{m}(G)$ esiste.

Se G è un insieme aperto e non-vuoto qualsiasi si può ancora considerare l'insieme dei numeri reali $\{m(F) \mid F \subseteq G,\ F \in \mathfrak{F}\mathfrak{E}\}$. Se tale insieme è limitato superiormente allora l'area o misura di G è per definizione l'estremo superiore di tale insieme; in simboli

$$m(G) = \sup \{m(F) \mid F \subseteq G,\ F \in \mathfrak{F}\mathfrak{E}\}.$$

Se tale insieme *non* è limitato superiormente si dice che G ha area $+\infty$. Per esempio $G = (a, b) \times \mathbf{R}$ e $G = \mathbf{R}^2$ hanno area $+\infty$.

In questo modo abbiamo definito la misura di ogni insieme aperto $G \subseteq \mathbf{R}^2$.

Si possono ancora verificare le proprietà A.1-A.4; inoltre l'area del rettangolo aperto $(a, b) \times (c, d)$ è data da $(b-a)(d-c)$.

Sia ora K un insieme chiuso (tale cioè che $\mathbf{R}^2 \setminus K$ sia aperto) e limitato, e quindi contenuto in un quadrato Q_h. L'area di K è l'estremo inferiore delle misure delle figure elementari che contengono K; in simboli

$$m(K) = \inf \{m(F) \mid K \subseteq F,\ F \in \mathfrak{F}\mathfrak{E}\}.$$

Tale estremo inferiore esiste sempre per l'assioma III di $\mathbf{R}$ poiché ogni $m(F)$ è ≥ 0. Gli insiemi chiusi e limitati sono quindi insiemi misurabili, per i quali valgono le proprietà A.1-A.5.

Sia ora E un qualunque insieme limitato.

Definiamo la misura esterna $m_e(E)$ come l'estremo inferiore delle misure degli insiemi aperti G che contengono E; in simboli

$$m_e(E) = \inf \{m(G) \mid G \text{ aperto},\ E \subseteq G\}.$$

Tale estremo inferiore esiste *sempre* per l'assioma di continuità di $\mathbf{R}$. Definiamo poi la misura interna di E come l'estremo superiore delle misure degli insiemi chiusi e limitati K contenuti in E; in simboli

$$\boldsymbol{m_i}(E) = \sup \{m(K) \mid K \subseteq E,\ K \text{ chiuso e limitato}\}.$$

Tale estremo superiore esiste sempre per l'assioma di continuità di $\mathbf{R}$ poiché E è limitato e quindi $E \subseteq Q_h$ ed allora $K \subseteq F \subseteq Q_h$ ed $m(K) \leq 4h^2$.

Perveniamo cosí alla definizione fondamentale: l'insieme limitato E è misurabile se la sua misura interna coincide con la sua esterna; in tal caso il numero $m(E) = \boldsymbol{m_i}(E) = m_e(E)$ è detto area (o anche misura piana) di E.

L'estensione al caso di un insieme E *non*-limitato si ha dicendo che l'in-

sieme non-limitato E è misurabile se per ogni h intero ≥ 1 risulta $E \cap Q_h$ misurabile. Se poi $\{m(E \cap Q_h) \mid h \text{ intero } \geq 1\}$ è un insieme di numeri reali limitato superiormente allora si pone per definizione $m(E) = \sup\{m(E \cap Q_h) \mid h$ intero $\geq 1\}$. Se invece $\{m(E \cap Q_h) \mid h \text{ intero } \geq 1\}$ non è un insieme limitato superiormente, allora si dice che l'insieme misurabile E ha misura $+\infty$. Ci sono insiemi piani limitati e non misurabili: un esempio può essere costituito dal seguente «pettine per pidocchi». Sia $E = \{(x, y) \mid 0 \leq x \leq 1$ ove se x è razionale, allora $0 \leq y \leq 1$ e se x non è razionale, allora $0 \leq x \leq 2\}$. È possibile vedere che ogni K è contenuto in $[0, 1] \times [0, 1]$ ed ogni G contiene $[0, 1] \times [0, 2]$ e quindi $m_i(E) = 1$, $m_e(E) = 2$.

Tenendo conto di quanto detto si ricava che la famiglia $\mathfrak{M}$ degli insiemi misurabili e la misura cosí definite rispondono al nostro obiettivo.

Se $E \in \mathfrak{M}$ è tale che $m(E) = 0$ si dice che E è trascurabile. Tali sono, per esempio, gli insiemi formati da un numero finito di punti. Anche un insieme formato da un numero finito di segmenti è trascurabile, giacché per ogni $\varepsilon > 0$ esiste una figura elementare di area minore di ε che contiene un tale insieme. È infine trascurabile l'insieme formato dai punti del perimetro di un poligono, di una circonferenza o di una ellisse, ecc. Nel contesto dell'area, come si può notare, abbiamo una teoria che dà il correlato preciso della frase di Dieudonné citata all'inizio del § 3.3.

Si tratta ora di vedere come calcolare nella pratica l'area degli insiemi misurabili; il lettore può rendersi conto immediatamente che la definizione data è assai poco maneggevole, ad esempio cercando di calcolare l'area di $E_k = \{\langle x, y\rangle \mid 0 \leq x \leq b \text{ e } 0 \leq y \leq x^k\}$ con k intero ≥ 2 fissato, oppure l'area del cerchio $S_2 = \{\langle x, y\rangle \mid x^2 + y^2 < 1\}$. La poca maneggevolezza è dovuta al fatto che si utilizza nella sostanza il metodo di esaustione (per il calcolo dell'area di S_2 si veda appunto la tavola 20).

Il calcolo delle primitive fornisce invece uno strumento estremamente potente e maneggevole per il calcolo delle aree; a tale fine premettiamo ancora qualche definizione. Sia f una funzione reale definita in $[a, b]$ con $f(x) \geq 0$; si dice rettangoloide chiuso di base $[a, b]$ relativo alla funzione f l'insieme

$$R_f = \{\langle x, y\rangle \mid a \leq x \leq b \text{ e } 0 \leq y \leq f(x)\}.$$

È naturale chiedersi per quali funzioni ≥ 0 risulti R_f insieme misurabile; l'esempio del «pettine per pidocchi» coincide con R_f ove sia

$$f(x) = \begin{cases} 1 & \text{per } x \text{ razionale} \\ 2 & \text{per } x \text{ irrazionale} \end{cases}$$

e quindi R_f non è misurabile.

Se l'insieme R_f è misurabile e l'area di R_f è finita, tale area viene indicata con il simbolo $\int_a^b f(t)\, dt$ (che viene detto integrale definito fra a e b di f); si dice pure che la funzione f è integrabile nell'intervallo $[a, b]$.

Un'utile condizione sufficiente per la misurabilità di R_f (e quindi per l'integrabilità di f fra a e b) è fornita dal teorema di Riemann: sia $f(x)$ una funzione

≥ 0 definita in $[a, b]$; se f è monotona e limitata in $[a, b]$, allora f è integrabile (e cioè R_f è misurabile con area finita).

Si dimostra pure che se la funzione $f(x)$ è continua in tutto l'intervallo $[a, b]$ allora R_f è misurabile. Data una tale funzione f possiamo quindi definire la funzione integrale di f

$$(2) \qquad R_f(x) = \int_a^x f(t)\, dt;$$

le proprietà dell'integrale permettono di verificare che $R_f(x)$ è continua in tutto l'intervallo $[a, b]$, è ivi derivabile e vale inoltre $D\, R_f(x) = f(x)$. $R_f(x)$ è dunque una primitiva di $f(x)$. Indicando con $F(x)$ una qualunque primitiva di $f(x)$ si ha dunque la formula fondamentale del calcolo integrale dovuta a Torricelli

$$(3) \qquad \int_a^b f(x)\, dx = F(b) - F(a),$$

che lega intimamente il calcolo delle aree al calcolo differenziale.

A titolo d'esempio definiamo in modo rigoroso la funzione logaritmo usando la teoria dell'integrazione. Consideriamo a tal fine la funzione $F(x) = \int_1^k dt/t$; risulta allora $F(1) = 0$, $F(x_1 x_2) = \int_1^{x_1 x_2} dt/t = \int_1^{x_1} dt/t + \int_{x_1}^{x_1 x_2} dt/t = F(x_1) + F(x_2)$ giacché $\int_{x_1}^{x_1 x_2} dt/t = \int_1^{x_2} ds/s$ (ove poniamo $s = x_1 t$: è questo un caso particolare della cosiddetta regola di integrazione per sostituzione). Inoltre la funzione $F(x)$ è ovviamente strettamente crescente in $(0, +\infty)$ e ivi convessa verso il basso (il suo codominio è $\mathbf{R}$). Tale funzione per definizione è detta logaritmo naturale di x e viene indicata col simbolo $\log_e x$ o piú brevemente $\log x$. La funzione inversa è continua monotona strettamente crescente: si tratta della funzione esponenziale; il numero e è definito implicitamente da $\int_1^e dt/t = 1$. In modo analogo si consideri la funzione, definita per $u \in \mathbf{R}$, $\vartheta(u) = 2\int_0^u dt/(1+t^2)$. Si tratta di una funzione dispari e crescente; definito allora

$$(4) \qquad \pi = 4\int_0^1 \frac{dt}{1+t^2}$$

risulta $\lim_{u \to \pm\infty} \vartheta(u) = \pm\pi$. Utilizzando la funzione inversa $u(\vartheta)$ definita in $-\pi < \vartheta < \pi$ si assume per definizione

$$\sin\vartheta = \frac{1 - u^2(\vartheta)}{1 + u^2(\vartheta)} \qquad \cos\vartheta = \frac{2u(\vartheta)}{1 + u^2(\vartheta)}$$

che vengono prolungate per continuità in $\vartheta = \pm\pi$ ponendo

$$\cos(\pm\pi) = \lim_{\vartheta \to \pm\pi} \cos\vartheta = -1, \qquad \sin(\pm\pi) = \lim_{\vartheta \to \pm\pi} \sin\vartheta = 0.$$

Le funzioni cosí definite si possono quindi prolungare per periodicità a $\mathbf{R}$. Ed è poi agevole ricavare le usuali formule di trigonometria e di derivazione:

il calcolo trigonometrico trova in questo contesto una delle sue piú naturali collocazioni. Concludiamo osservando che la formula (4) può essere usata per approssimare il valore di π; basta infatti approssimare numericamente tale integrale definito, per esempio usando proprio la definizione di integrale definito.

Non possiamo certo sviluppare nemmeno per grandi linee il calcolo differenziale/integrale; ricordiamo solo il teorema della media che è ovvia conseguenza della nostra definizione di area: se $m \leq f(x) \leq M$ in $[a, b]$ si ha per ogni funzione $g(x) \geq 0$ in $[a, b]$

$$m \int_a^b g(t)\, dt \leq \int_a^b f(t)\, g(t)\, dt \leq M \int_a^b g(t)\, dt$$

che costituisce il fondamento teorico del «*procedimento piú importante dell'analisi* per ottenere maggiorazioni o minorazioni» [Dieudonné 1968, p. 42].

La teoria dell'integrazione fu radicalmente rinnovata da Lebesgue (1902) che forní uno strumento molto flessibile e adatto a nuove esigenze di ricerca (calcolo delle probabilità, analisi funzionale, calcolo delle variazioni, ecc.): il concetto di misura ivi utilizzato è un'estensione estremamente potente di quello da noi presentato, in quanto i soli esempi di insiemi non misurabili nel senso di Lebesgue sono ottenuti in modo non costruttivo utilizzando l'assioma della scelta (esempio di Vitali). Sfruttando i metodi introdotti da Cohen per le dimostrazioni di indipendenza, Solovay ha trovato un modello della teoria degli insiemi (con una versione indebolita dell'assioma della scelta) in cui tutti gli insiemi del piano sono misurabili nel senso di Lebesgue.

3.6. Calcolo coi numeri complessi.

Il calcolo coi numeri complessi deve la sua origine, come abbiamo già accennato nel § 2.4 a un dilemma che si presentò agli algebristi del Rinascimento: per affrontare certi problemi, per esempio la risoluzione dell'equazione $x^2+1=0$, veniva naturale introdurre l'unità «immaginaria» $\sqrt{-1}$ e tuttavia appariva poco intuitivo e scarsamente rigoroso ammettere nella famiglia dei numeri enti del genere, non rappresentabili sulla retta numerica. Solo gradatamente (cfr. del resto il passo di Cauchy riportato nel § 3.3) i matematici riuscirono a superare le loro prevenzioni nei riguardi degli immaginari e a stabilire per essi un'apposita dottrina matematica, scoprendo che la radice quadrata di -1 può essere combinata con i numeri reali, dando luogo ai numeri «complessi» e che questi obbediscono alle solite regole del calcolo. Oggi il calcolo coi complessi è uno strumento di uso universale sia nella matematica pura sia nelle applicazioni alle scienze empiriche e all'ingegneria; è la chiave per lo studio dei numeri primi, si applica a svariati problemi di aeronautica, d'idrodinamica, di progettazione dei circuiti elettronici, ecc.

È interessante, dunque, alla luce di quanto detto piú sopra, ricordare il modo in cui Cauchy introdusse i numeri complessi nei suoi *Exercices d'analyse et de physique mathématique* [1847].

Come il lettore sa fin dalla scuola secondaria, è possibile sommare, sottrarre, moltiplicare, dividere tra loro non solo i numeri, ma anche i polinomi a coefficienti numerici: è possibile anche – l'idea è già presente nelle *Disquisitiones* di Gauss – sviluppare, sulla falsariga della teoria delle congruenze per gli interi relativi (§ 2.4), una teoria delle congruenze per polinomi, poniamo, a coefficienti reali. Se A e B sono due polinomi nell'indeterminata x, l'estensione ai polinomi dell'usuale algoritmo euclideo della divisione permette di determinare univocamente, per B diverso dal polinomio nullo, due polinomi Q e R tali che $A=BQ+R$ (ove il grado di R è minore di quello di B): due polinomi A_1 e A_2 si diranno *congruenti modulo un polinomio* B se divisi per B dànno il medesimo resto R (e scriveremo ancora $A_1 \equiv A_2 \bmod B$). Il lettore da $A_1=BQ_1+R_1$ e $A_2=BQ_2+R_2$ può agevolmente ricavare $A_1+A_2 \equiv R_1+R_2 \bmod B$ e $A_1A_2 \equiv R_1R_2 \bmod B$.

Possiamo ora intendere il ragionamento di Cauchy. Nulla vieta di dividere un qualsiasi polinomio a coefficienti reali $f(x)$ per il polinomio x^2+1: si ha allora $f(x) \equiv a+bx \bmod x^2+1$ poiché il resto è di grado minore del divisore e a e b sono reali (grazie all'algoritmo euclideo). Se quindi $g(x)$ è un altro polinomio e $g(x) \equiv c+dx \bmod x^2+1$, abbiamo subito

$$f(x)+g(x) \equiv (a+c)+(b+d)\,x \qquad \bmod x^2+1$$
$$f(x) \times g(x) \equiv (ac-bd)+(ad+bc)\,x \qquad \bmod x^2+1$$

e se $g(x)$ non è congruo a 0 modulo x^2+1 si mostra pure che $g(x)$ «ha un inverso» $h(x)$, cioè esiste un polinomio $h(x)$ tale che $h(x)\,g(x)$ è congruo a 1 modulo x^2+1. Cosí le scritture formali $a+bx$, $c+dx$ si combinano come i numeri complessi ampiamente utilizzati nella pratica: tali numeri possono dunque venir identificati con le classi di polinomi congruenti mod x^2+1.

Il lettore ritrova i numeri complessi nella scrittura che gli è piú familiare, sostituendo al segno x il segno i.

Cauchy osserva: «La lettera i cessa di rappresentare il segno simbolico $\sqrt{-1}$ che ripudiamo completamente e che abbandoniamo senza rimpianto, perché non sappiamo che cosa con tale segno si voglia denotare o che significato si debba attribuire a esso. Al contrario con la lettera i denotiamo una quantità reale [*sic!*] ma indeterminata e sostituendo al segno $=$ il segno $\equiv$ trasformiamo quel che una volta si chiamava equazione immaginaria in una equivalenza algebrica relativa alla variabile i e al divisore i^2+1» [1847, pp. 84 sg.]. Coerentemente con il giudizio espresso nel *Cours d'Analyse* (riportato nel § 3.3), Cauchy di nuovo condanna in nome del rigore la pratica degli algebristi del suo tempo e mostra di aver ben assimilato la lezione di Gauss. L'approccio prettamente calcolistico degli *Exercices* pone a sua volta le premesse di un profondo rinnovamento dell'algebra nel senso di maggior generalità e rigore. Basti dire che nel 1882 Kronecker, prendendo spunto proprio dal procedimento di Cauchy, fa dell'aggiunzione di indeterminate a un corpo la pietra angolare della sua trattazione della teoria dei numeri algebrici e si rivela perfettamente consapevole del fatto che le «indeterminate» sostengono, nella sua teoria, solo il ruolo di elementi di base di un'algebra e non quello di variabili nel

senso dell'analisi. Tale idea verrà ripresa cinque anni dopo nel contesto del suo ambizioso programma inteso alla ristrutturazione dell'intera matematica ripudiando tutto quanto non è riducibile a operazioni algebriche su numeri interi (ricordiamo il motto riportato nel § 2.3: «Dio ha creato i numeri naturali, tutto il resto è opera dell'uomo»).

C'è un altro aspetto dei numeri complessi che ci pare interessante richiamare qui. Quel che rappresentava un rompicapo prima della trattazione rigorosa di Cauchy era il fatto – per usare le parole di Eulero [1768] – che «tutti i numeri concepibili sono maggiori, minori o uguali a o ed è dunque chiaro che le radici quadrate di numeri negativi non rientrano tra i numeri possibili». Eulero ne concludeva che si trattava di «numeri impossibili»; in una presentazione rigorosa appare immediato che il sistema dei complessi forma un corpo non ordinato (soddisfa cioè gli assiomi I.1-I.6 ma non quelli II.1-II.5 del § 2.4).

Tuttavia l'ottica maggiorare/minorare/approssimare si adatta anche al calcolo coi complessi; per rendercene conto utilizziamo l'interpretazione geometrica dovuta a Wessel (1797), Argand (1806) e Gauss (1811, lettera a Bessel).

Nel piano cartesiano è possibile infatti associare al numero complesso $z=a+bi$ il punto di coordinate $\langle a, b\rangle$, o anche il vettore che congiunge l'origine con tale punto. L'addizione dei numeri complessi si interpreta allora immediatamente come l'addizione dei due vettori; per quanto riguarda la moltiplicazione rimandiamo alla figura 11.

La lunghezza del vettore $\langle a, b\rangle$ è per definizione il modulo del numero

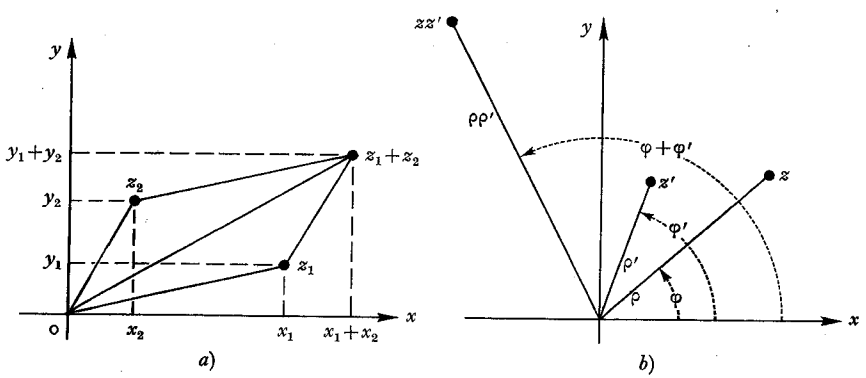


Figura 11.

Addizione e moltiplicazione di due numeri complessi. *a*) Regola del parallelogramma per trovare la somma z_1+z_2 di $z_1=x_1+y_1i$ e $z_2=x_2+y_2i$; *b*) moltiplicazione dei due numeri z e z'. L'angolo formato dal semiasse positivo x e dalla retta oz fornisce il cosiddetto argomento di z che indichiamo con φ; con ρ indichiamo il modulo di z che può scriversi allora $z=\rho(\cos\varphi+i\sin\varphi)$; nella moltiplicazione, come si vede, i moduli si moltiplicano e gli argomenti si sommano.

complesso z ed è usualmente notata $|z|$. Dal teorema di Pitagora si ha immediatamente

$$|z|=\sqrt{a^2+b^2}$$

ove il segno $\sqrt{\ }$ denota la radice quadrata aritmetica (cfr. § 3.3).

Il modulo è dunque una applicazione di **C** in **R** che gode delle seguenti proprietà:

N.1. $|z|\geq 0$ e $|z|=0$ se e solo se $z=0$.

N.2. $|z+w|\leq|z|+|w|$.

N.3. $|zw|=|z|\,|w|$.

Se $z=a+0i=a$ allora $|z|$ coincide con l'usuale valore assoluto di a.

Grazie a tali proprietà è possibile definire l'analogo degli intervalli (i cosiddetti dischi) e generalizzare senza difficoltà la nozione di limite e le sue conseguenze.

In particolare la funzione $f: U\to\mathbf{C}$ (dove U è un aperto di **C**) è derivabile (od olomorfa) in $z_0\in U$ se esiste $a\in\mathbf{C}$ tale che per ogni $h\in\mathbf{C}$ con $z_0+h\in U$ si abbia $f(z_0+h)=f(z_0)+ah+h\varepsilon(h)$ con $\varepsilon(h)$ infinitesimo per h tendente a zero.

Con la rappresentazione precedente è naturale scrivere $f(z)=u(x, y)+iv(x, y)$ se $z=x+iy$; un teorema fondamentale asserisce che f è derivabile se e solo se le funzioni $u(x, y)$ e $v(x, y)$ sono differenziabili (come funzioni delle variabili reali x, y) e valgono le equazioni di Cauchy-Riemann

$$\frac{\partial u}{\partial x}=\frac{\partial v}{\partial y}\qquad\frac{\partial u}{\partial y}=-\frac{\partial v}{\partial x}.$$

La proprietà fondamentale delle funzioni $f: U\to\mathbf{C}$ è che l'olomorfia di f in U equivale al fatto che f sia analitica in U e cioè sviluppabile in serie di potenze in un intorno di ogni suo punto.

Se f è olomorfa in tutto **C** allora f deve essere costante (teorema di Liouville). Da tale teorema è possibile ricavare che ogni polinomio a coefficienti complessi o è identicamente nullo o ammette almeno uno zero in **C** (teorema fondamentale dell'algebra: Gauss, 1799).

Il teorema fondamentale dell'algebra chiude il problema, cosí sentito dagli algebristi del Cinquecento (Cardano, Tartaglia), di estendere il sistema dei numeri in modo che ogni equazione algebrica ammetta ivi soluzione.

Tale teorema è ormai un classico esempio di teorema esistenziale ma non costruttivo; approssimare numericamente le soluzioni di una equazione algebrica può essere un'impresa difficile anche usando i piú sofisticati e potenti mezzi di calcolo numerico.

3.7. Equazioni differenziali ordinarie.

Molti dei fenomeni oggetto di studio nelle varie branche della scienza e della tecnologia sono caratterizzati dalla loro evoluzione durante un intervallo

di tempo $I \subseteq \mathbf{R}$. Tali fenomeni sono generalmente detti processi (cfr. l'articolo «Applicazioni» di questa stessa *Enciclopedia*, § 1.1) e, opportunamente schematizzati, sono oggetto di indagine matematica. La prima tappa di questa schematizzazione consiste nell'individuare l'insieme M di tutti gli stati possibili, cioè il cosiddetto spazio delle fasi. Un processo durante l'intervallo I è allora una famiglia di applicazioni g^t di M in M; per ogni $x \in M$ l'insieme $\{g^t x \mid t \in I\}$ viene detto orbita e l'applicazione $t \to \varphi(t) = g^t x$ di I in M è detta movimento di x durante il processo.

Un processo è detto deterministico se tutto il suo passato e tutto il suo futuro sono univocamente determinati dal suo stato presente (nel caso in cui $I = \mathbf{R}$ e g^t è un gruppo a un parametro di applicazioni di M si parla di flusso). Per esempio nella meccanica classica si studia il movimento di un sistema di punti materiali il cui passato e il cui futuro sono univocamente definiti dalla posizione e velocità all'istante t_0 di ogni punto del sistema. Nella meccanica quantistica invece si studia una situazione assai piú complicata in cui la conoscenza dello stato del sistema all'istante t_0 determina soltanto la probabilità che in un tempo successivo il sistema sia in un certo sottoinsieme di M. La propagazione del calore è un processo in cui il presente determina il futuro ma non il passato.

Un processo è di dimensione finita se il numero dei parametri necessari per descriverne lo stato è finito, e cioè se lo spazio delle fasi ha dimensione finita.

Per esempio in meccanica classica un sistema di n punti materiali è descritto da $6n$ parametri (in effetti per ogni punto 3 parametri ne individuano la posizione e 3 parametri la velocità), un sistema di n corpi rigidi liberi è descritto da $12n$ parametri; naturalmente se tali sistemi sono vincolati allora la dimensione dello spazio delle fasi diminuisce.

Un processo è poi detto differenziabile se il suo spazio delle fasi M può essere munito di una struttura di varietà differenziabile (definita nell'articolo «Applicazioni», § 3.6) e se i suoi cambiamenti di stato nel tempo (e cioè la legge di evoluzione g^t) sono definiti da funzioni differenziabili. Anche in questo caso un esempio è fornito dal movimento di un sistema di punti materiali, quando questo avvenga senza urti.

Lo strumento matematico sostanzialmente ideato da Newton per lo studio dei processi deterministici, di dimensione finita e differenziabili, è costituito dalla teoria delle equazioni differenziali ordinarie. In meccanica classica infatti il movimento di un sistema può essere descritto mediante equazioni differenziali ordinarie che traducono la legge fondamentale della meccanica forza = = massa × accelerazione. Altri esempi di processi deterministici, di dimensione finita e differenziabili, sono la disintegrazione radioattiva e la riproduzione di batteri in un brodo di coltura (in quantità sufficiente). In entrambi i casi lo spazio delle fasi è unidimensionale: lo stato del processo è definito nel primo caso dalla quantità restante di materia radioattiva e nel secondo dal numero di batteri. Naturalmente la forma dell'equazione differenziale ordinaria che descrive il processo concreto (ed il fatto stesso che tale processo sia deterministico, di dimensione finita e differenziabile) può essere stabilita solo sperimentalmente e quindi solo con un certo grado di approssimazione.

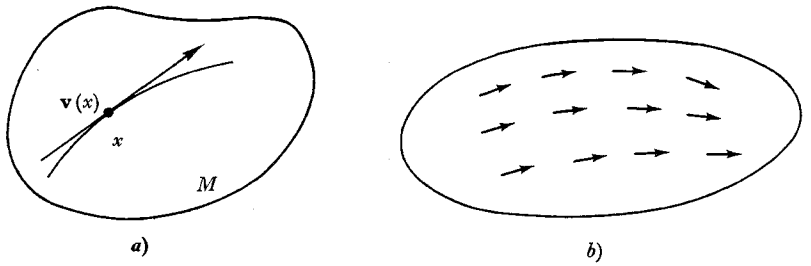


Figura 12.
Rappresentazione schematica di un vettore velocità (*a*) e di un campo di vettori (*b*).

Ad ogni processo di dimensione finita e differenziabile è possibile associare un campo di vettori $\mathbf{v}$, detto il campo delle velocità locali del processo, nel modo seguente: se $x = \varphi(t_0) \in M$ allora $\mathbf{v}(x) = (d\varphi/dt)|_{t=t_0}$; scriveremo talvolta $\dot{x}$ od x' invece di $(d\varphi/dt)|_{t=t_0}$ (fig. 12).

Illustriamo le definizioni precedenti con alcuni esempi.

Esempio 1.

È noto sperimentalmente che la velocità di disintegrazione radioattiva è proporzionale alla quantità di materia x. Lo spazio delle fasi è quindi la semiretta $M = \{x \mid x > 0\}$, mentre la legge di disintegrazione radioattiva si scrive $\dot{x} = -kx$ per cui $\mathbf{v}(x) = -kx$, $k > 0$.

Esempio 2.

La caduta libera di un grave da un'altezza poco elevata è tale che la sua accelerazione è costante (legge di Galileo). Lo spazio delle fasi è rappresentato dal piano (x_1, x_2) dove x_1 è l'altezza e x_2 la velocità (fig. 13), la legge sperimentale si esprime con le formule $\dot{x}_1 = x_2$, $\dot{x}_2 = -g$ (ove $-g$ è l'accelerazione di gravità) e quindi il campo della velocità $\mathbf{v}$ ha componenti $v_1 = x_2$ e $v_2 = -g$.

Esempio 3.

Le piccole oscillazioni del pendolo semplice sono descritte da un intorno M dell'origine del piano x_1, x_2 ove x_1 è l'angolo dalla verticale e x_2 la velocità angolare. Per la legge di Galileo l'accelerazione è proporzionale all'angolo per cui risulta $\dot{x}_1 = x_2$, $\dot{x}_2 = -kx_1$ con $k = l/g$ ove l è la lunghezza del pendolo e g l'accelerazione di gravità. Risulta quindi $\mathbf{v} = \langle v_1, v_2 \rangle$ con $v_1 = x_2$, $v_2 = -kx_1$; l'origine delle coordinate è tale che $\mathbf{v} = \mathbf{0}$, si tratta per definizione di un punto singolare del campo di vettori (cfr. fig. 14).

Esempio 4.

Una descrizione piú precisa delle oscillazioni del pendolo (non necessariamente di piccola ampiezza) conduce alla legge $\dot{x}_1 = x_2$, $\dot{x}_2 = -k \sin x_1$. Come

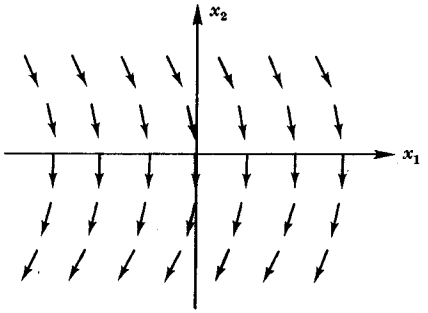
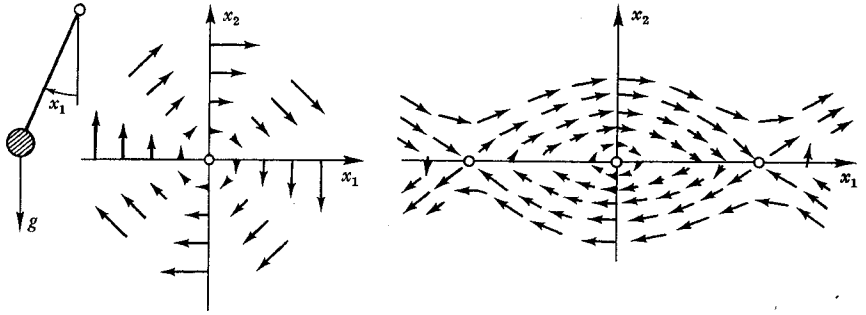


Figura 13.
Piano di fase della caduta libera di un grave.



a) *b)*

Figura 14.
Rappresentazione schematica delle piccole oscillazioni (*a*) e del campo delle velocità (*b*) del pendolo.

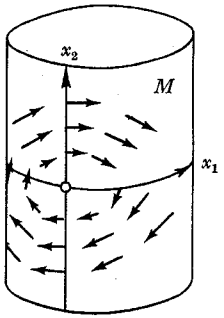


Figura 15.
Spazio delle fasi cilindriche per il pendolo.

spazio delle fasi può assumersi tutto il piano (x_1, x_2) (fig. 13) o, meglio per la periodicità della funzione sin, la superficie del cilindro (fig. 15).

Illustriamo quindi alcuni aspetti della teoria delle equazioni differenziali ordinarie.

Sia $f(t, x)$ una funzione definita in $I \times H$ e a valori in E dove I è un intervallo aperto di $\mathbf{R}$ e H un aperto dello spazio di Banach E (per la nozione di spazio di Banach, si veda anche il § 3.8). Una funzione differenziabile u definita nell'intervallo $\mathcal{J} \subseteq I$ ed a valori in H è detta soluzione dell'equazione differenziale ordinaria

$$\dot{x} = f(t, x) \tag{5}$$

se per ogni $t \in \mathcal{J}$ si ha

$$u'(t) = f(t, u(t)).$$

Se $E = \mathbf{R}$ si ha una equazione differenziale ordinaria scalare, se $E = \mathbf{R}^n$ si ha un sistema di n equazioni differenziali ordinarie.

Si dice spazio delle fasi esteso dell'equazione (5) il prodotto cartesiano $\mathbf{R} \times E$ e si dice curva integrale di (5) ogni soluzione di tale equazione.

Nel caso $E = \mathbf{R}$ lo spazio delle fasi esteso è la striscia $\mathbf{R} \times H$; in tale caso il campo delle direzioni corrispondenti all'equazione (5) è ottenuto tracciando per ogni punto $\langle t, x \rangle$ di $I \times H$ la retta di coefficiente angolare $f(t, x)$ (e cioè la retta che forma un angolo con l'asse x la cui tangente vale $f(t, x)$). Una curva integrale, in ognuno dei suoi punti, è tangente al campo delle direzioni.

Il problema di Cauchy consiste nel determinare una soluzione di (5) che verifichi la condizione iniziale $u(t_0) = x_0$.

Osserviamo che ogni soluzione del problema di Cauchy verifica l'equazione integrale

$$u(t) = x_0 + \int_{t_0}^{t} f(s, u(s))\, ds.$$

Nel caso particolare in cui f non dipende da x la risoluzione dell'equazione differenziale si riduce al calcolo della primitiva di f. Nel latino di Eulero [1768, p. 1]: «Calculus integralis est methodus, ex data differentialium relatione inveniendi relationem ipsarum quantitatum».

Il teorema di esistenza di Cauchy, sotto l'ipotesi che f sia derivabile con continuità, assicura per ogni $t_0 \in \mathcal{J}$ ed ogni $x_0 \in H$ l'esistenza e l'unicità in un intervallo $\mathcal{J} = (t_0 - \delta, t_0 + \delta)$ della soluzione del problema di Cauchy. Tale soluzione dipende con continuità dai dati $\langle t_0, x_0 \rangle$.

Si tratta di un teorema di esistenza locale e cioè in un piccolo intervallo di tempo; sotto ulteriori ipotesi per f si hanno risultati di esistenza globale e cioè in tutto I.

Una possibile dimostrazione del teorema di Cauchy consiste nel costruire con procedimento iterativo la successione

$$u_0(t) = x_0$$
$$u_1(t) = x_0 + \int_{t_0}^{t} f(s, u_0(s))\, ds$$
$$\cdots\cdots\cdots\cdots$$
$$u_n(t) = x_0 + \int_{t_0}^{t} f(s, u_{n-1}(s))\, ds$$
$$\cdots\cdots\cdots\cdots$$

e nel dimostrare che tale successione ammette un limite: è il metodo di Peano-Picard.

Nel caso in cui $E = \mathbf{R}$ (od $E = \mathbf{R}^n$) è possibile approssimare la curva integrale passante per $\langle t_0, x_0 \rangle$ mediante una successione di poligonali. Il piú semplice modo è quello di Eulero; precisamente, posto $t_m = t_0 + mh$ (ove $h > 0$ è il passo del metodo) si approssima il valore $u(t_m)$ della soluzione esatta con u_m ove la successione u_m è definita da

$$(6) \qquad \begin{cases} u_0 = x_0 \\ u_{m+1} = u_m + h\, f(t_m, u_m) \qquad m = 0, 1, \ldots \end{cases}$$

I punti $\langle u_m, t_m \rangle$ geometricamente si interpretano come i vertici di una poligonale che approssima la curva integrale che costituisce la soluzione del problema di Cauchy.

Le formule (6) possono interpretarsi anche come approssimazione dell'equazione integrale; infatti si ha

$$u(t_{m+1}) - u(t_m) = \int_{t_m}^{t_{m+1}} f(s, u(s))\, ds$$

ed allora (6) si ottiene approssimando l'integrale a secondo membro. Proprio a partire da tale interpretazione si possono costruire metodi numerici assai precisi (i cosiddetti metodi di Runge-Kutta).

Un quesito naturale in questo contesto è quello della convergenza della soluzione ottenuta con il metodo di Eulero alla soluzione esatta di (5) quando il passo h tende a zero. Tale questione rientra nella problematica generale affrontata nell'articolo «Approssimazione» di questa stessa *Enciclopedia* e il risultato dell'esempio 8 (I, p. 787) assicura tale convergenza; cfr. anche oltre, § 4.8.

In connessione con i problemi di meccanica delle vibrazioni, particolare sviluppo ha avuto lo studio dei problemi periodici in cui $I = \mathbf{R}$, f è una funzione periodica in t e si cerca una soluzione periodica; si tratta di problemi che grande influenza hanno avuto nello sviluppo dell'analisi non-lineare degli ultimi decenni.

Concludiamo questa sezione ricordando che un'altra applicazione fondamentale delle equazioni differenziali ordinarie si ha nella descrizione della configurazione spaziale di mezzi continui, soggetti a opportune distribuzioni di forze, nei quali predomini una sola dimensione spaziale.

Si consideri in particolare il problema di un'asta rettilinea, in assenza di sollecitazione esterna, diretta come l'asse x, su cui agiscono soltanto due forze opposte dirette anch'esse come l'asse x, cosí come è indicato nella figura 16. Se $y = f(x)$ rappresenta l'asta in condizione di equilibrio, tale funzione verifica l'equazione differenziale (detta equazione della linea elastica piana)

$$(7) \qquad \frac{y''}{(1 + y'^2)^{3/2}} + \frac{f_A}{k} y = 0$$

con le condizioni al contorno $y(0) = y(l) = 0$. k è per un'asta omogenea una costante > 0 che dipende solo dalla natura elastica dell'asta e dalla forma e dalla dimensione della sezione trasversale del corpo tridimensionale che rappresentiamo con la linea elastica monodimensionale. Un integrale particolare della (7) è evidente: $y = 0$, in corrispondenza al quale l'asta non muta la sua configurazione rettilinea.

Se il carico f_A non è eccessivo e se la lunghezza l dell'asta non è troppo grande rispetto a k, l'asse dell'asta resta rettilineo e la deformazione si riduce a una contrazione proporzionale a f_A che corrisponde alla sola soluzione $y = 0$. Se però f_A/k è grande abbastanza si ha anche una soluzione non nulla che corrisponde a un'asta incurvata (nel caso di una colonna o di un pilastro in una costruzione muraria si ha una catastrofe – il crollo della costruzione! – poiché allora la soluzione $y = 0$ corrisponde a un equilibrio instabile e dunque ha significato fisico la soluzione non nulla).

Ha quindi grande importanza determinare il primo carico critico f_A^* in corrispondenza del quale si ha la prima biforcazione. La determinazione della configurazione dell'asta condusse Eulero (1744) a intraprendere lo studio degli integrali ellittici

$$\int_{\varphi}^{\pi/2} \sqrt{1 - k^2 \sin^2 \vartheta}\, d\vartheta \qquad \int_{\varphi}^{\pi/2} (1 - k^2 \sin^2 \vartheta)^{-1/2}\, d\vartheta.$$

In questo modo si può ricavare che il primo valore critico è $f_A^* = \pi^2 k / l^2$; tale risultato può venir agevolmente ottenuto applicando la moderna teoria della biforcazione.

Lo studio degli integrali ellittici fu poi ripreso da Legendre (1825), Abel (1828), Jacobi (1832) e infine da Riemann che nel 1857 rivoluzionò l'argomento

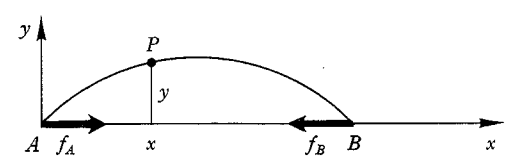


Figura 16.
Asta soggetta a due forze opposte.

introducendo considerazioni geometriche e topologiche completamente nuove che sfociarono nel celebre teorema di Riemann-Roch che è uno dei capisaldi della moderna geometria algebrica.

Le funzioni ellittiche ottenute da Jacobi e Abel «invertendo» gli integrali ellittici ed estendendone la definizione al campo complesso si sono rivelate assai importanti e significative nell'ambito della geometria algebrica e della teoria dei numeri, grazie anche ai fondamentali contributi di Weierstrass.

3.8. Problemi ben posti.

Di una data situazione fisica possono venir costruiti modelli matematici diversi, in funzione delle «contraddizioni principali» in esame, dipendenti in generale dalla nostra conoscenza piú o meno approfondita della realtà.

In ogni caso «un problema matematico che voglia corrispondere alla realtà fisica dovrebbe soddisfare i seguenti requisiti fondamentali: 1) la soluzione esiste; 2) la soluzione è determinata univocamente; 3) la soluzione dipende con continuità dai dati (condizione di stabilità).

«Il primo requisito esprime la condizione logica che alla soluzione non sia imposto troppo, e cioè proprietà tra loro incompatibili.

«Il secondo requisito implica la completezza del problema: incertezza e ambiguità devono essere escluse se non inerenti alla situazione fisica. (Vi sono casi in cui l'unicità non è un requisito adeguato. Per esempio, nel caso di autovalori multipli esistono intere famiglie di soluzioni del problema agli autovalori).

«Il terzo requisito, particolarmente stringente, è necessario affinché la formulazione matematica descriva fenomeni naturali osservabili. I dati sperimentali non possono venir concepiti come fissati rigidamente; il semplice processo di misurazione comporta piccoli errori. Per esempio, valori assegnati delle coordinate spaziali o temporali sono sempre stabiliti entro un certo margine di precisione. Pertanto possiamo pensare che un problema matematico corrisponda in modo realistico a fenomeni fisici solo nel caso in cui una variazione sufficientemente piccola dei dati implica una modificazione arbitrariamente piccola della soluzione. Questo requisito di "stabilità" è essenziale non solo per problemi dotati di senso nella fisica matematica, ma anche per i metodi di approssimazione. Un qualunque problema che soddisfi i nostri tre requisiti sarà detto problema *ben posto*» [Courant e Hilbert 1962, p. 227].

La nozione di problema ben posto, introdotta originariamente da Hadamard (1921), può essere considerata come espressione del determinismo. Cosí il teorema di Cauchy ricordato nel § 3.7 significa appunto che il problema dei valori iniziali è ben posto.

I modelli di molti fenomeni fisici sono descritti da un sistema di equazioni a derivate parziali, eventualmente non-lineari, con le relative condizioni al contorno e iniziali; il loro studio è in generale complicato, anche se è naturale pensare che, in quanto tali modelli sono stati costruiti in modo «aderente» alla realtà, i problemi da risolvere siano ben posti.

Questo è proprio ciò che accade nei modelli che esamineremo e che corrispondono a situazioni semplici; esistono peraltro fenomeni piú complicati (per esempio in fluidodinamica) di cui si ignora se il modello costruito sia aderente alla realtà. In tale caso lo studio matematico, o almeno numerico, del modello proposto diventa fondamentale anche nella valutazione della sua aderenza alla realtà.

Osserviamo infine che da un punto di vista strettamente matematico per dire che il problema è ben posto vanno individuati in modo corretto gli spazi funzionali in cui si cerca la soluzione e quelli in cui variano i dati (cfr. quanto diremo oltre, dopo l'esempio 3).

Diamo ora alcuni esempi.

Esempio 1 (tratto dall'elasticità lineare).

Consideriamo una membrana elastica Ω (isotropa e con tensione uniforme $T>0$) fissata alla frontiera Γ sul piano x, y. Se la membrana è sottoposta a una distribuzione di forze verticali di densità $f(x, y)$ subirà uno spostamento verticale $u(x, y)$. Nell'ambito della elasticità lineare lo spostamento incognito u può esser ottenuto considerando diverse formulazioni del problema.

Prima formulazione. Lo spostamento u è la soluzione del problema al contorno

$$(8)\qquad \begin{cases} -T\left(\dfrac{\partial^2 u}{\partial x^2}+\dfrac{\partial^2 u}{\partial y^2}\right)=f & \text{in } \Omega \\ u=0 & \text{su } \Gamma \end{cases}$$

Seconda formulazione. Si definisca lo spazio degli spostamenti ammissibili $V=\{v \mid v$ è «regolare» in Ω e $v=0$ su $\Gamma\}$ e l'energia totale corrispondente a uno spostamento ammissibile

$$I(v)=\text{energia di deformazione}+\text{energia delle forze esterne}=$$
$$=\frac{1}{2}\int_\Omega T\left\{\left(\frac{\partial v}{\partial x}\right)^2+\left(\frac{\partial v}{\partial y}\right)^2\right\}dx\,dy-\int_\Omega fv\,dx\,dy.$$

Il principio di minima energia dice che la soluzione u è quello spostamento ammissibile che rende minima l'energia totale e cioè è soluzione del problema

$$\begin{cases} u\in V \\ I(u)\leq I(v) & \text{per ogni } v\in V. \end{cases}$$

Terza formulazione. Il lavoro virtuale dello spostamento v rispetto allo spostamento u è dato dalla «forma bilineare»

$$a(u, v)=\int_\Omega T\left\{\frac{\partial u}{\partial x}\frac{\partial v}{\partial x}+\frac{\partial u}{\partial y}\frac{\partial v}{\partial y}\right\}dx\,dy$$

mentre il lavoro virtuale delle forze esterne rispetto allo spostamento v è dato dalla «forma lineare»

$$(f, v) = \int_\Omega fv\, dx\, dy.$$

La soluzione u deve essere uno spostamento ammissibile tale che

$$\begin{cases} u \in V \\ a(u, v) = (f, v) \qquad \text{per ogni } v \in V. \end{cases}$$

Accanto alle formulazioni precedenti, in termini esclusivamente di spostamenti, altre sono possibili in termini di sforzi o di deformazioni, basate su altri principî variazionali.

Affinché le formulazioni precedenti diventino completamente rigorose è necessario precisare la regolarità di v ed f in modo che $I(v)$ abbia minimo e non solamente estremo inferiore.

Il problema (8) è noto come problema di Dirichlet e l'esistenza del minimo di $I(v)$ è nota come principio di Dirichlet. Nello studio della seconda formulazione è cruciale distinguere fra estremo inferiore e minimo. In effetti, mentre è facile trovare classi di funzioni per cui $I(v)$ è limitato inferiormente, non è altrettanto evidente determinare classi in cui tale minimo sia raggiunto (Weierstrass); è questo un caso particolare della problematica che è alla base del calcolo delle variazioni.

Supponiamo per semplicità $f \in L^2(\Omega)$ e cioè tale che $\int_\Omega |f|^2\, dx\, dy < +\infty$ ove l'integrale è quello di Lebesgue. Vogliamo solo indicare una classe di funzioni per le quali $I(v)$ ammette minimo, almeno per Ω limitato e a frontiera sufficientemente regolare (per esempio poligonale). Si tratta dello spazio di Sobolev $H_0^1(\Omega)$ che si ottiene completando $C_\Gamma^1(\bar{\Omega}) = \{v \mid v$ è continuamente derivabile in un intorno aperto di $\bar{\Omega}$ e risulta $v = 0$ su $\Gamma\}$ rispetto alla norma della energia

$$\|v\|_{1,\Omega} = \left(\int_\Omega \left\{ \left(\frac{\partial v}{\partial x}\right)^2 + \left(\frac{\partial v}{\partial y}\right)^2 \right\} dx\, dy \right)^{1/2}.$$

$H_0^1(\Omega)$ è uno spazio di Hilbert ed è allora possibile dimostrare (Weyl, Lax-Milgram) che il problema nella seconda formulazione ammette una e una sola soluzione che dipende con continuità dal dato f assumendo $V = H_0^1(\Omega)$.

La terza formulazione non è altro che la condizione di Eulero di estremo corrispondente alla seconda.

Assai piú delicato è il problema della prima formulazione e di una sua eventuale equivalenza alla terza (e quindi alla seconda). In generale tali formulazioni possono non essere equivalenti nel senso che la soluzione u della seconda (o terza) formulazione può non ammettere derivate parziali seconde; per tale motivo la terza formulazione viene considerata una formulazione debole della prima. Se si considerano le derivate nel senso della teoria delle distribuzioni allora l'equivalenza è assicurata, ma si pone il problema della regolarità

della soluzione di (8). Ritroviamo questa problematica alla base di molte ricerche recenti di analisi volte a risolvere i problemi XIX, XX, XXIII di Hilbert [per i problemi hilbertiani [1900] e in particolare per queste tematiche, cfr. Browder 1976, pp. 26-27, 27-28, 29-34, e ancora pp. 507-24, 525-35, 611-28].

Esempio 2 (tratto dalla propagazione del calore).

L'evoluzione del campo di temperatura (adimensionale) $\vartheta(x, t)$ in una sbarra omogenea unidimensionale di lunghezza $l > 0$ è retta dall'equazione

$$(9) \qquad \frac{\partial \vartheta}{\partial t} - a \frac{\partial^2 \vartheta}{\partial x^2} = Q(x, t) \qquad \text{per } x \in (0, l)$$

ove $a > 0$ è un parametro assegnato e Q designa la densità di quantità di calore prodotto. All'equazione si devono aggiungere la condizione iniziale $\vartheta(x, 0) = \vartheta_0(x)$, e la condizione al contorno, che per semplicità assumeremo $\vartheta(0, t) = \vartheta(l, t) = 0$ per $t \in [0, T]$.

Del problema testé proposto si può dare la seguente formulazione variazionale: determinare la funzione $\vartheta(t)$ definita per $t \in [0, T]$ e a valori nello spazio $V = H_0^1(0, l)$ tale che

$$\int_0^l \left\{ \frac{\partial \vartheta}{\partial t} r + \frac{\partial \vartheta}{\partial x} \frac{\partial r}{\partial x} \right\} dx = \int_0^l \psi r\, dx \qquad \text{per ogni } r \in V \text{ e } \vartheta(0) = \vartheta_0.$$

Anche in questo caso se $Q \in L^2((0, l) \times (0, T))$ si verifica che il problema cosí formulato è ben posto.

Illustriamo ora il cosiddetto metodo di Fourier nel caso particolare in cui $Q = 0$, la cui idea di fondo consiste nel cercare la soluzione come superposizione di soluzioni particolari del tipo $X(x)$, $T(t)$. Si ottiene allora da (9) che $X(x)$ e $T(t)$ devono verificare la relazione

$$\frac{T'(t)}{a\, T(t)} = \frac{X''(x)}{X(x)} = \lambda$$

con λ costante reale; quindi $T(t)$ e $X(x)$ verificano $T'(t) = \lambda\, a\, T(t)$, $X''(x) = \lambda X(x)$. Tenendo conto delle condizioni al contorno otteniamo una soluzione $X(x)$ non nulla solo per $\lambda = -(k^2\pi^2/l^2)$ con k intero ≥ 1. Appare allora naturale cercare la soluzione $\vartheta(x, t)$ nella forma

$$(10) \qquad \vartheta(x, t) = \sum_{k=1}^{\infty} \vartheta_k \sin \frac{k\pi x}{l}\, e^{-k^2(a\pi^2/l^2)t}$$

ove i coefficienti ϑ_k sono ottenuti dalla relazione

$$(11) \qquad \vartheta(x, 0) = \sum_{k=1}^{\infty} \vartheta_k \sin \frac{k\pi x}{l} = \vartheta_0(x).$$

Fu proprio la ricerca delle soluzioni scritte in questo modo a condurre Joseph Fourier a studiare la possibilità di rappresentare una funzione come somma di una serie trigonometrica [1822]. Tale problematica si è quindi naturalmente biforcata in queste due nuove questioni:

I) data la funzione $u(x)$ definita nell'intervallo $(0, l)$ è possibile determinare una successione di numeri a_k tali che $u(x)=\sum_{k=1}^{\infty} a_k \sin k\pi x/l$? (Si tratta della cosiddetta analisi armonica);

II) data una successione di numeri a_k esiste una funzione $u(x)$ definita in $(0, l)$ tale che $u(x)=\sum_{k=1}^{\infty} a_k \sin k\pi x/l$? (È il problema della sintesi spettrale).

Si può rispondere alle domande I) e II) solo quando il contesto ci permette di definire la convergenza di una serie di funzioni; ambiti naturali per tali questioni sono i cosiddetti spazi di Banach e di Hilbert di cui ora ricordiamo la definizione. Uno spazio normato E sul corpo K (con $K=\mathbf{R}$ oppure $K=\mathbf{C}$) è uno spazio vettoriale su K nel quale sia definita una norma e cioè una applicazione che a ogni e di E associa un numero reale denotato $\|e\|_E$ (o solo $\|e\|$) che gode delle proprietà

N'.1. $\|e\|\geq 0$ e $\|e\|=0$ se e solo se $e=0$

N'.2. $\|e+f\|\leq\|e\|+\|f\|$ per ogni $e, f\in E$

N'.3. $\|\lambda e\|=|\lambda|\,\|e\|$ per ogni $\lambda\in K$ e per ogni $e\in E$.

Un confronto di N'.1 - N'.3 con N.1-N.3 del § 3.6 mostra immediatamente che $\mathbf{C}$ si può concepire come uno spazio normato su $\mathbf{R}$ prendendo come norma del numero complesso z il suo modulo. In generale alla norma si può associare una distanza $d(e, f)=\|e-f\|$. Se poi per tale norma lo spazio è completo, nel senso che per esso vale una proprietà analoga alla proprietà V del § 3.3, si dice allora che E è uno spazio di Banach. Uno spazio di Hilbert E su K è infine uno spazio di Banach in cui la norma verifica la legge del parallelogramma

$$\|x+y\|^2+\|x-y\|^2=2(\|x\|^2+\|y\|^2) \qquad \text{per ogni } x, y\in E$$

(cfr. del resto la figura 11a). In tale spazio possiamo allora definire il prodotto scalare di x e y ponendo

$$(x\mid y)=\frac{1}{2}\|x+y\|^2-\frac{1}{2}\|x\|^2-\frac{1}{2}\|y\|^2 \qquad \text{nel caso } K=\mathbf{R}$$

$$(x\mid y)=\frac{1}{4}(\|x+y\|^2-\|x-y\|^2+i\|x+iy\|^2-i\|x-iy\|^2) \qquad \text{nel caso } K=\mathbf{C}.$$

Non possiamo approfondire qui tali argomenti, di fondamentale importanza per lo sviluppo della matematica del XX secolo. Ricordiamo solo che nell'ambito delle serie di Fourier fra gli spazi piú significativi sono lo spazio di Banach $L^1(0, l)$ formato da tutte le funzioni (a valori reali o complessi) integrabili secondo Lebesgue e munito della norma

$$\|f\|_{L^1(0,l)}=\int_0^l |f(x)|\,dx$$

e lo spazio di Hilbert $L^2(0, l)$ formato da tutte le funzioni (a valori reali o complessi) integrabili secondo Lebesgue e munito del prodotto scalare

$$(f\mid g)=\int_0^l f(x)\,g(x)\,dx \qquad \left(\text{risp. } (f\mid g)=\int_0^l f(x)\,\overline{g(x)}\,dx\right).$$

Riprendendo allora il nostro esempio: se $\vartheta_0\in L^2(0, l)$ allora la (11) permette di determinare i coefficienti ϑ_k con la formula

$$\vartheta_k=\frac{2}{l}\int_0^l \vartheta_0(x)\sin\frac{k\pi x}{l}\,dx$$

e tali coefficienti verificano la condizione $\sum_{k=1}^{\infty}|\vartheta_k|^2<+\infty$.

È allora facile dimostrare che la serie (10) e tutte le sue derivate sono convergenti per ogni $t\geq 0$ e che vale inoltre $\lim_{t\to+\infty}\vartheta(x, t)=0$, risultato che s'interpreta fisicamente dicendo che la temperatura di una sbarra non scaldata e con gli estremi mantenuti a temperatura nulla tende a zero per $t\to+\infty$. Per $t<0$ la serie (10) è divergente a meno che la successione dei coefficienti ϑ_k converga molto rapidamente a zero per $k\to\infty$. Ciò significa che il problema retrogrado è in generale mal posto (esempio di Hadamard).

Concludiamo osservando che i problemi dell'analisi armonica e della sintesi spettrale sono stati oggetto di profondi studi nel corso degli ultimi centocinquant'anni. Ci basta qui ricordare che fu proprio in connessione con tali studi che per Georg Cantor, motivato in particolare da ricerche di Riemann, maturò a partire dal 1870 la necessità di una precisa classificazione dei sottoinsiemi di $\mathbf{R}$ destinata a segnare una svolta anche nella problematica stessa dei fondamenti della matematica.

Esempio 3 (tratto dalla propagazione delle onde).

Le onde sonore in un fluido perfetto compressibile sono movimenti vibratori di piccola ampiezza; le equazioni della meccanica dei fluidi si possono allora linearizzare intorno alla posizione di equilibrio e tutte le incognite possono essere espresse in funzione della sola funzione φ (detta il potenziale delle velocità) che verifica l'equazione delle onde (dove $c>0$ è la velocità del suono)

$$\frac{\partial^2\varphi}{\partial t^2}-c^2\left(\frac{\partial^2\varphi}{\partial x^2}+\frac{\partial^2\varphi}{\partial y^2}+\frac{\partial^2\varphi}{\partial z^2}\right)=0. \tag{12}$$

Infatti, nota φ si ricavano

$$v_1=\frac{\partial\varphi}{\partial x} \qquad v_2=\frac{\partial\varphi}{\partial y} \qquad v_3=\frac{\partial\varphi}{\partial z} \qquad \rho=-\rho_0\frac{\partial\varphi}{\partial t}$$

dove ρ_0 è la velocità del fluido non perturbato e $\mathbf{v}=\langle v_1, v_2, v_3\rangle$ è la velocità dell'onda.

L'equazione (12) è fondamentale nei fenomeni vibratori ed è stata introdotta da d'Alembert nel 1746 proprio nello studio delle vibrazioni di un corpo elastico.

Nel caso particolare in cui tutte le quantità dipendono dalla sola coordinata x (e cioè il movimento è omogeneo nel piano y, z: si tratta della cosiddetta onda piana) l'equazione (12) diventa

$$\frac{\partial^2\varphi}{\partial t^2}-c^2\frac{\partial^2\varphi}{\partial x^2}=0 \tag{13}$$

(equazione delle corde vibranti) ed è allora possibile vedere che almeno formalmente la soluzione generale è $\varphi(x, t)=f_1(x-ct)+f_2(x+ct)$ con f_1, f_2 arbitrarie. Si tratta naturalmente di una soluzione classica (detta soluzione di d'Alembert) del problema nel caso in cui f_1 ed f_2 siano derivabili due volte; «se esse sono solo continue o una volta derivabili si ha tuttavia l'impressione che la funzione φ definita sopra sia pur sempre una soluzione, in un senso opportuno, dell'equazione delle corde vibranti. Di qui l'idea di soluzione generalizzata» [Schwartz 1972, p. 179]. Tale idea introdotta da Leray (1934), Sobolev (1936), Friedrichs (1939), venne sviluppata in modo completamente rigoroso nella teoria delle distribuzioni di Schwartz (1945).

Osserviamo che $f_1(x-ct)$ rappresenta un'onda piana che si propaga nel senso positivo dell'asse x, mentre $f_2(x+ct)$ rappresenta un'onda che si propaga in senso inverso.

Consideriamo dapprima l'equazione (13) con $x\in\mathbf{R}$ e cerchiamo una soluzione che verifichi le condizioni iniziali $\varphi(x, 0)=\varphi_0(x)$ e $(\partial\varphi/\partial t)(x, 0)=\varphi_1(x)$ ove φ_0 e φ_1 sono funzioni definite per $x\in\mathbf{R}$ (il caso in cui φ rappresenta lo spostamento verticale della corda è detto caso della corda infinita). Tali condizioni iniziali permettono di fissare le funzioni f_1 e f_2; precisamente si ha

$$\begin{cases} f_1(x)=\frac{1}{2}\varphi_0(x)-\frac{1}{2c}\int_0^x\varphi_1(z)\,dz \\ f_2(x)=\frac{1}{2}\varphi_0(x)+\frac{1}{2c}\int_0^x\varphi_1(z)\,dz \end{cases} \tag{14}$$

da cui si ricava la soluzione

$$\varphi(x, t)=\frac{\varphi_0(x-ct)+\varphi_0(x+ct)}{2}+\frac{1}{2c}\int_{x-ct}^{x+ct}\varphi_1(z)\,dz. \tag{15}$$

La formula (14) fornisce la cosiddetta soluzione classica se φ_0 è due volte derivabile con continuità in $\mathbf{R}$ e φ_1 è una volta derivabile con continuità.

Dalla (15) si vede come il comportamento in $P_0=\langle x_0, t_0\rangle$ di φ sia determinato solamente dal comportamento di φ_0 e di φ_1 nell'intervallo (x_0-ct_0, x_0+ct_0). Nel piano x, t le due famiglie di rette $x\pm ct=\text{cost}$ sono dette caratteristiche dell'equazione (13) e il triangolo individuato da P_0 e dalle due caratteristiche che escono da P_0 è detto triangolo di influenza (cfr. fig. 17).

Nel caso di una corda finita di lunghezza l, fissata alle estremità, le cui ascisse sono $x=0$ e $x=l$ l'equazione (13) e le condizioni iniziali vanno considerate solo per $0\leq x\leq l$. Affinché il problema sia ben posto si aggiungono le condizioni agli estremi $\varphi(0, t)=0$ e $\varphi(l, t)=0$, per $t\geq 0$.

La soluzione del problema è ancora data nella forma di d'Alembert con f_1 e f_2 individuate da (14); ma c'imbattiamo in una difficoltà in quanto $\varphi_0(x)$ e $\varphi_1(x)$ sono definite solo per $0\leq x\leq l$. Si tratta allora di prolungare tali funzioni al di fuori di tale intervallo; ciò può essere fatto, tenendo conto delle condizioni al contorno, ponendo $\varphi_0(-x)=-\varphi_0(x)$ per $-l\leq x\leq 0$, e $\varphi_1(-x)=-\varphi_1(x)$ per $-l\leq x\leq 0$; e quindi per periodicità di periodo $2l$ su tutta la retta. Ne consegue che gli estremi $x=0$ e $x=l$ riflettono l'onda di spostamento e tale riflessione è legata al cambiamento di segno dello spostamento.

Nel piano x, t si ha la situazione indicata in figura 18. I punti della regione I corrispondono a punti della corda raggiunti da impulsioni provenienti solo da punti interni; nei punti delle regioni II e III vi è anche l'influenza della riflessione dell'onda dovuta all'estremità; nelle regioni IV, V, VI si ottengono onde che hanno subito varie riflessioni.

Un esempio particolarmente semplice di applicazione di tale procedimento si ha nel caso della «corda pizzicata» che all'istante iniziale è fissata in uno dei suoi punti senza velocità (e cioè $\varphi_1=0$). Posto $\tau=l/c$, nella figura 19 è indicata la forma successiva della corda negli istanti $t=0$, $t=\tau/4$, $t=\tau/2$, $t=3\tau/4$, $t=\tau$.

Un argomento attualmente al centro di profondi studi è quello della propagazione delle singolarità: se i dati iniziali φ_0 e φ_1 hanno una singolarità in x_0, le singolarità di φ si propagano a partire da x_0 secondo le leggi dell'ottica geometrica? La risposta relativamente semplice nel caso dell'equazione (13) diventa assai piú complicata nel caso di problemi misti iperbolici di carattere generale e di domini $\Omega\subset\mathbf{R}^n$ con $n\geq 2$.

Osserviamo che i problemi precedenti sono attualmente affrontati, in genere, nel contesto della teoria degli operatori lineari fra opportuni spazi di Banach (o di Hilbert) sul corpo reale o complesso. Indicando con K indifferentemente $\mathbf{R}$ o $\mathbf{C}$, ricordiamo che $A: E\to F$ è detta applicazione od operatore lineare (con E, F Banach o Hilbert) se $A(x+y)=Ax+Ay$ per ogni $x, y\in E$, e $A(\lambda x)=\lambda Ax$ per ogni $x\in E$ e ogni $\lambda\in K$.

L'operatore lineare A è detto poi continuo (o limitato) se esiste $M>0$ tale che $\|Ax\|_F\leq M\|x\|_E$ per ogni $x\in E$; il piú piccolo M per cui tale maggiorazione è vera è detto norma di A e viene indicato con $|||A|||$; gli operatori continui da E in F formano uno spazio di Banach per tale norma.

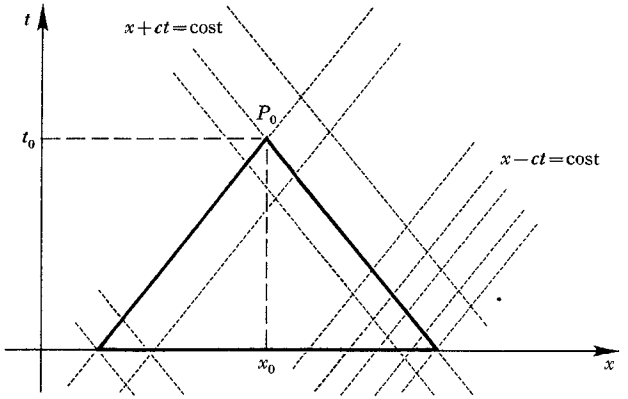


Figura 17.
Le caratteristiche e il triangolo di influenza.

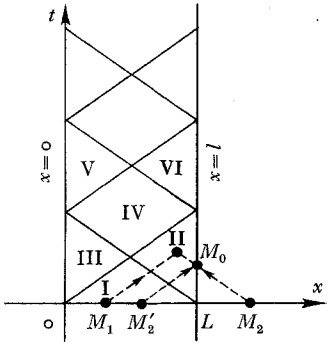


Figura 18.
Diagramma nel piano x, t delle regioni di influenza dei dati iniziali e delle condizioni al contorno.

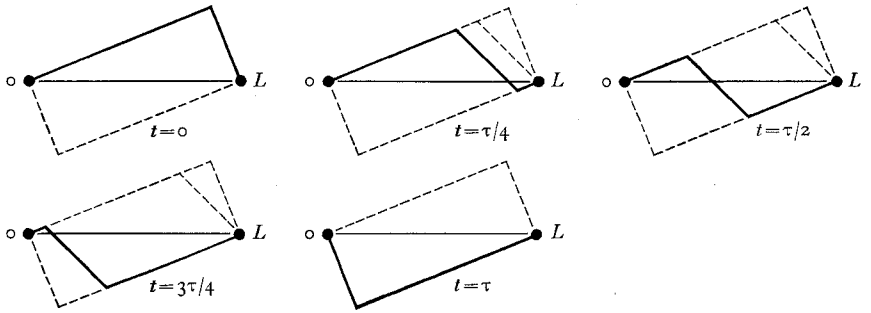


Figura 19.
Corda pizzicata.

I nostri problemi possono allora scriversi nella forma seguente (una volta scelti opportunamente gli spazi E, F e l'operatore A): dato $b \in F$ trovare $x \in E$ tale che $Ax = b$. Le condizioni di unicità e stabilità del problema ben posto si dimostrano in generale provando una maggiorazione a priori del tipo

$$\|x\|_E \leq L\|b\|_F \tag{16}$$

con L che non dipende né da x né da b. Per esempio nel caso del problema di Dirichlet (cfr. l'esempio 1) si dimostra abbastanza agevolmente la maggiorazione $\|u\|_{H_0^1(\Omega)} \leq L\,\|f\|_{L^2(\Omega)}$ e quindi il problema ha certo unicità e stabilità.

Osserviamo peraltro che per provare la maggiorazione (16) basterebbe provare che esiste l'operatore A^{-1} inverso di A e che A^{-1} è continuo da F in E.

Vogliamo concludere questa sezione sui problemi ben posti ricordando che «questo ideale di determinismo matematico-causale è stato gradualmente eroso dal confronto con la realtà fisica. Fenomeni non lineari, teoria quantistica e infine il sorgere di potenti metodi numerici hanno mostrato che i problemi "ben posti" sono ben lungi dall'essere gli unici che riflettano in modo appropriato i fenomeni reali. Fino a ora, tuttavia, sono stati ottenuti scarsi progressi matematici nell'importante compito di risolvere o anche solo d'identificare e formulare quei problemi che non sono "ben posti" ma sono tuttavia importanti e motivati da situazioni concrete» [Courant e Hilbert 1962, p. 230].

L'obiettivo proposto da Courant è stato perseguito negli ultimi anni, in cui si sono sempre piú studiati i cosiddetti «problemi mal posti» (per esempio problemi inversi, problemi di controllo, problemi di frontiera libera, ecc.). Tuttavia alcuni di questi problemi si rivelano ben posti quando una piú accurata analisi del problema fisico fa apparire nel modello delle condizioni supplementari (per esempio del tipo ottimizzazione di qualche funzionale come nei problemi di controllo, ecc.). La dicotomia principale/secondario tra le varie contraddizioni e negli aspetti di una singola contraddizione non è fissa, ma slitta: nel caso in questione le difficoltà matematiche fanno emergere l'inadeguatezza del modello, retroagiscono sulla stessa schematizzazione della struttura fisica ponendo l'esigenza di una schematizzazione piú fine.

4. *Il calcolo numerico.*

4.1. Il punto di vista predittivo. Il programma di Fourier.

Talete previde un'eclisse e divenne uno dei Sette Savi; Descartes nei *Principia Philosophiae* [1644] affermava che sappiamo che le nostre ipotesi sono corrette quando possiamo da esse «dedurre tutte le altre piú particolari, alle quali non avevamo badato» (trad. it. vol. II, pp. 139-40). Leibniz da parte sua scriveva a Conring (1678) che «la miglior garanzia di un'ipotesi... è che con il suo aiuto si possono fare predizioni anche intorno a fenomeni ed esperimenti non previsti» [citato e discusso in Lakatos 1970, trad. it. pp. 198 sg.]. Nel pensiero occidentale almeno, è comune a tradizioni intellettuali, per altri aspetti molto diverse, l'abbinamento del potere predittivo e di quello esplicativo delle teorie. Senza dubbio

furono la formulazione della meccanica newtoniana e il corrispondente sviluppo dell'analisi nell'età moderna a far rifiorire il calcolo preventivo degli eventi naturali e con esso la fiducia nel «valore della scienza». Newton aveva espresso le sue leggi del moto e della gravitazione come equazioni differenziali. Laplace agli inizi dell'Ottocento enunciava un grandioso programma in cui tutta la conoscenza della realtà veniva modellata sul determinismo della meccanica celeste: anche «la curva descritta da una semplice molecola di aria o di vapore, è regolata con la stessa certezza delle orbite planetarie» [Laplace 1814, trad. it. p. 245]. Nel § 3.8, del resto, abbiamo visto come la nozione di problema ben posto riprenda proprio l'idea generale del determinismo matematico-causale.

Non c'è quindi da stupirsi del fatto che Comte, fondatore del positivismo francese, compendiasse le funzioni della scienza pura e di quella applicata nel motto «scienza significa previsione; previsione sinonimo d'azione» [Comte 1830-42, trad. it. p. 106], fondando l'efficacia di una tecnologia sul successo predittivo.

Una forte esigenza predittiva permane anche nelle piú drammatiche contrapposizioni della scienza degli ultimi due secoli (meccanica deterministica / meccanica quantistica, meccanica newtoniana / meccanica relativistica, ecc.) che hanno fatto emergere esigenze di elaborare schemi concettuali piú profondi. Non è casuale quindi che per esempio Karl Popper, pur guardando all'impresa scientifica da un'ottica fallibilista e antinduttivista, caratterizzi piú di un secolo dopo Comte la «logica della scoperta» come una *logic of tests* 'una logica dei controlli' e prospetti il progresso scientifico come aumento del contenuto empirico almeno parzialmente corroborato delle teorie [cfr. Popper 1959, 1972; Lakatos 1970; e l'articolo «Anticipazione» di questa stessa *Enciclopedia*].

La stessa caratterizzazione dei calcoli come sistemi formali nell'*Encyclopedia of Unified Science* (cfr. § 2.7) si estende in modo naturale alle scienze empiriche aggiungendo alla descrizione sintattica di un calcolo l'interpretazione intesa «in forma di regole semantiche»: cosí, per esempio, la meccanica del punto materiale è un calcolo *fisico* in questa particolare accezione: certi termini vengono scelti come primitivi, le leggi fondamentali della meccanica fungono da assiomi specifici e le regole semantiche specificano quel che i segni primitivi designano, per esempio la classe dei punti materiali, le tre coordinate spaziali di un punto materiale P al tempo t, la massa di P, la classe delle forze agenti su P al tempo t, ecc. [Carnap 1939, pp. 56 sgg.].

Caratterizzazioni di questo tipo adombrano l'idea piú generale di modello matematico di processi reali: un certo insieme di relazioni (algebriche, differenziali, integrali, ecc.) viene ritenuto rappresentativo dei fenomeni presi in considerazione e, detto in breve, fornisce numeri da mettere in confronto coi dati empirici, non bruti beninteso, ma filtrati attraverso sofisticati procedimenti di misurazione. Si tratta di definizioni di modello che si collocano su un piano di notevole astrazione: il controllo dello schema – o il vaglio stesso delle conseguenze delle ipotesi e delle semplificazioni introdotte – è, per esempio, fuori di ogni vincolo di tempo reale. «Diamo il nostro contributo all'edificio della conoscenza oggettiva come artigiani che costruiscono una cattedrale» [Popper 1959, trad. it. p. xv].

Se in quest'ottica un calcolo, in via di principio, deve terminare, ma non importa quando, nella tecnologia invece i vincoli di tempo si rivelano spesso essenziali. I modelli vanno risolti rapidamente proprio per poter fornire efficaci strumenti euristici a chi controlla il fenomeno, il quale se ne vale per prendere decisioni sulla conduzione del sistema stesso.

La gamma delle posizioni intermedie tra la concezione per cosí dire «oggettivista» (propria della fase spiegazione scientifica) e quella «strumentalista» (propria della fase realizzazione tecnologica) rappresenta l'esito di una concezione del calcolo che affonda le sue radici almeno nella mediazione ottocentesca tra l'immagine del sapere ereditata dagli autori illuministi dell'*Encyclopédie* e l'idea «positivista» che vede nella «rete matematica» uno schema per calcoli adeguati piuttosto che la chiave per intendere la natura profonda dei processi naturali. Cosí leggiamo agli esordi del *mathematical poem* (il termine è di Engels) di Joseph Fourier che «se i corpi sono collocati lontano da noi, nell'immensità dello spazio e se l'uomo vuole conoscere lo spettacolo dei cieli in epoche distanti un gran numero di secoli... è l'analisi matematica che può enunciare le leggi di questi fenomeni, rendendoceli presenti e misurabili» [1822, p. xxiv]. Ma «i risultati del calcolo» devono essere passibili di «interpretazione numerica», necessaria in tutte le applicazioni alle scienze naturali tanto che «si può dire che, nella misura in cui non la si è ottenuta, le soluzioni restano incomplete e inutili: la verità che ci si proponeva di scoprire è celata nelle formule di analisi tanto quanto prima lo era nello stesso problema fisico» [*ibid.*, p. 9]. Fourier delineava cosí un paradigma per la ricerca.

Questa prospettiva viene meno però una volta emerse le difficoltà insite nel tipo di equazioni usate per rappresentare matematicamente i fenomeni. Ne è un sintomo, nella seconda metà dell'Ottocento, lo slittamento del termine 'modello', che decade a sinonimo di espediente atto a rendere piú intuitiva l'immagine dei processi naturali. Mach offre sotto questo profilo passi esemplari (si veda per esempio il giudizio sul calcolo delle variazioni, ridotto a puro schema analogico [1883, trad. it. p. 468 e anche pp. 478-79]).

Perché riemerga appieno il paradigma di Fourier si deve attendere il nostro secolo: tale rinascita del resto si comprende solo alla luce delle profonde trasformazioni della produzione scientifica e tecnologica. Per esempio: «La teoria e la pratica della costruzione numerica delle soluzioni delle equazioni differenziali ordinarie ha ricevuto un impulso dalle richieste della tecnologia moderna, di cui l'esplorazione dello spazio è solo l'esempio piú cospicuo. La tecnologia spaziale senza metodi efficienti per risolvere le equazioni differenziali ordinarie è impensabile quanto la città di Los Angeles senza l'automobile» [Henrici 1963, p. vi].

4.2. «Metodi numerici» e «analisi numerica».

Le origini del «calcolo numerico» nell'accezione di questo paragrafo risalgono ovviamente a molto prima di Fourier. I Babilonesi possedevano ottime approssimazioni di $\sqrt{2}$ sin da dodici secoli prima che i Greci si convincessero

dell'incommensurabilità della diagonale con il lato del quadrato. Nella *Misura del cerchio* Archimede determina, verso il 250 a. C., la stima di π tra $3+10/71$ e $3+10/70$ (cfr. tav. 20). La «tavola delle corde» (funzioni trigonometriche) di Claudio Tolomeo (150 d. C.) costituisce già un'applicazione esemplare dei metodi numerici dell'epoca.

Ma non è il caso di continuare in una ricostruzione, anche per grandi linee, dello sviluppo di tali metodi dalla tarda antichità ai giorni nostri. Qui vogliamo ricordarne solo due tratti caratteristici, in un certo senso antitetici, in quanto l'uno inquadra gli aspetti della creatività nella scoperta matematica, mentre l'altro sembra concernere il lavoro di routine. Metodi teorici / dispositivi concreti: a questa opposizione rimanda la constatazione che l'esigenza di ottenere risposte numeriche ai piú svariati quesiti ha motivato spesso ardite innovazioni nell'analisi matematica, mentre, col diventare sempre piú complicati i problemi da risolvere, l'esecuzione materiale di calcoli numerici si è rivelata faccenda laboriosa, pesante e troppo spesso viziata da inesattezze. Proprio ciò ha stimolato l'invenzione e il perfezionamento di una vastissima gamma di strumenti materiali di calcolo, dalle prime calcolatrici da tavolo ai calcolatori elettronici moderni.

C'è dunque un profondo intreccio tecnologia/calcolo: per rendercene conto riprendiamo l'esempio di Carnap [1939] citato nel § 4.1 e supponiamo, piú in particolare, di studiare il moto di un proiettile quando siano assegnate posizione e velocità iniziali. Il procedimento piú opportuno per esprimere numericamente posizioni e velocità successive in funzione del tempo può benissimo dipendere dai mezzi materiali di cui disponiamo: se abbiamo solo carta e matita o magari anche un calcolatore elettromeccanico da tavolo organizziamo i calcoli in un certo modo: se disponiamo di un calcolatore elettronico, li organizziamo diversamente e possiamo inoltre utilizzare programmi già compilati eventualmente in nostro possesso, sfruttando le caratteristiche peculiari del nostro strumento. In casi del genere ci si trova di fronte a diverse vie possibili e tocca all'«analisi numerica» valutarle una per una.

L'attenzione ai mutamenti terminologici in genere è produttiva; lo è tanto piú in una enciclopedia che è condizionata dalla costellazione delle idee, dei linguaggi, dei testi in cui il progetto che la sottende viene a inscriversi e al contempo modifica col suo stesso apparire tale costellazione. 'Calcolo approssimato', 'metodi numerici' e simili fanno pensare a un semplice insieme di tecniche; invece 'analisi numerica', prima del 1950 locuzione praticamente sconosciuta, coll'aggettivo rivendica la propria specificità rispetto all'analisi *tout court*, col sostantivo ne sottolinea l'affinità, complessivamente richiama l'idea di una disciplina autonoma e omogenea.

«Nell'età pre-computer l'analisi numerica – cioè l'analisi pratica, com'era di solito chiamata – aveva, come disciplina matematica, ben pochi punti di contatto con l'analisi matematica cosí come era praticata dal matematico puro. Provare l'esistenza di un oggetto matematico, come la soluzione di qualche equazione funzionale ed esibire quello stesso oggetto, per esempio costruendo una tabella di valori numerici della soluzione, erano due cose del tutto differenti. Anche quando l'esistenza era dimostrata con metodi costruttivi, i calcoli che di fatto richiedevano queste dimostrazioni costruttive d'esistenza erano di regola troppo pesanti per qualsiasi impiego pratico. Di conseguenza, quando si trattava di soluzioni numeriche, si insisteva soprattutto sui problemi che permettevano, in una forma o nell'altra, una soluzione esplicita. Se una soluzione del genere non era disponibile, si ricorreva a tecniche numeriche solo con grande riluttanza e ben piccolo era l'incentivo per un'indagine matematica rigorosa di tali metodi. Questa situazione è mutata radicalmente con l'avvento dei dispositivi digitali elettronici. Molte tecniche costruttive dell'analisi classica, concepite in origine soprattutto come strumenti per dimostrare teoremi, possono ora venir messe all'opera con grande facilità per ottenere risposte numeriche. Conseguentemente c'è stato un ritorno di interesse per tali algoritmi costruttivi generali, e si può dire *cum grano salis* che l'analisi numerica è oggi – o, almeno, diventerà presto – lo studio dettagliato degli algoritmi costruttivi dell'analisi. Contemporaneamente gli esperti di problemi computazionali si dimostrano sempre piú sensibili... al grado di costruttività di un dato algoritmo. Per essi fa dunque differenza se qualche oggetto matematico esiste solo sulla base dell'assioma di scelta, o per il teorema di Arzelà, o come limite di una successione di Cauchy i cui elementi possono venir costruiti mediante i razionali» [Henrici 1963, pp. 1-2].

Il riferimento allo strumento di calcolo è cruciale: le normali calcolatrici da tavolo possono solo dispensare dal compiere le operazioni elementari (il lavoro essenziale – raccolta di risultati intermedi, decisioni relative al proseguimento del calcolo, ecc. – resta compito dell'uomo); la progettazione di macchine in grado di pianificare il calcolo a somiglianza del soggetto umano ha invece aperto nuove strade. Ciò che era adombrato nel progetto (1822; cfr. tav. 29) di Babbage – l'*analytical engine*, capace di eseguire calcoli al di là delle normali limitazioni umane – è stato realizzato solo dopo la seconda guerra mondiale. Il 1946 è l'anno di nascita ufficiale di ENIAC (*Electronic Numerical Integrator and Calculator*), il calcolatore programmabile dovuto agli sforzi congiunti di Eckert, Mauchly, Goldstine e Neumann, progettato originariamente per calcolare tabelle di tiro, ma agevolmente modificabile in modo da poter eseguire altri calcoli, come la soluzione di equazioni alle derivate parziali, ecc.: è ormai tradizione che questa data segni l'inizio di quella che con una certa enfasi è stata battezzata «la rivoluzione del calcolatore» e di cui oggi cogliamo nella pratica quotidiana l'aspetto di costume legato all'utilizzazione dei calcolatori tascabili come fenomeno di massa.

Uomo/macchina: una contrapposizione/interazione di fondo che sottende per il calcolo la contrapposizione/interazione tra la matematica del matematico «puro» e la «matematica dell'ingegnere». Per dirla con John von Neumann, preparare un problema per un moderno calcolatore digitale è un po' come fornire istruzioni a un soggetto umano non troppo intelligente che, munito di una calcolatrice da tavolo, esegue tutti i compiti assegnatigli senza avere altre comunicazioni con l'esterno, finché presenta le risposte ai quesiti posti. Questa caratterizzazione può ancora apparire riduttiva (in certe versioni piú sofisticate la

macchina può, per cosí dire, «apprendere», «dialogare» con l'utente, ecc.), ma qui ci basta per comprendere che non tutti i metodi di calcolo naturali per il soggetto umano si rivelano adatti a un calcolatore e viceversa. E, detto ancora un po' schematicamente, occorre pure ricordare che, in confronto all'uomo, il calcolatore è piú rapido e piú economico: la tecnologia segna quindi un potenziamento del «calcolo» e introduce nuove esigenze (per esempio, di tecniche piú raffinate per analizzare il problema, che va scomposto in un numero finito di passi prima di essere affidato alla macchina).

Di nuovo possiamo apprezzare la dialettica della coppia astratto/concreto. Bene tale dialettica è colta in Turing [1950]: i dispositivi di calcolo digitali sono «macchine a stati discreti», in quanto si «muovono a salti o a scatti improvvisi da uno stato definito a un altro» (trad. it. p. 125); ma già cosí definiti sono delle astrazioni, in quanto la fisica che ne fonda la tecnologia è una fisica del continuo (pensiamo, per esempio, ai circuiti elettrici cui è fatto cenno nel § 2.6, ove supponevamo che un interruttore fosse *o* chiuso *o* aperto, *prescindendo* dalle inevitabili posizioni intermedie). D'altro canto l'analisi classica incentrata sull'idea di continuità solo apparentemente fornisce reti matematiche adeguate, anche se in linea puramente teorica gli schemi che essa offre sembrano riflettere piú fedelmente processi continui reali. Tale ingenua concezione non si adatta al paradigma delineato da Fourier (a parte la questione, peraltro di grandissima importanza, degli schemi piú adatti per lo studio di situazioni in cui forze e motivazioni che cambiano gradualmente portano a bruschi cambiamenti: vedi per esempio la teoria matematica delle catastrofi). L'impostazione del calcolo tipo maggiorare/minorare/approssimare (cfr. § 3.4) fa invece dei «metodi numerici» un potente strumento di approfondimento sia di questioni tradizionalmente ritenute «scienza pura» sia di questioni altrettanto rigidamente confinate nell'ambito «scienza applicata e tecnologia».

4.3. Problemi computazionali.

Una prima limitazione di un modello matematico, per esempio, è connessa con la disponibilità dei dati d'ingresso e si comprende subito che il successo di una simulazione matematica dipende notevolmente dal tipo d'informazione disponibile (del resto, anche l'Intelligenza di Laplace [1814] deve pur essere informata sulle condizioni iniziali dell'universo), informazione che dipende in modo notevole dalle conoscenze di base. Una seconda limitazione concerne direttamente gli strumenti di calcolo e la questione degli errori: sono fonti d'errore la sostituzione di variabili continue con variabili discrete, il troncamento di procedimenti matematici in linea di principio infiniti, il necessario arrotondamento dei valori numerici con cui si opera, come avremo modo di vedere tra poco.

Ciò premesso, possiamo reinterpretare la richiesta di Fourier come quella di tramutare un problema «scientifico» in un «problema computazionale», che definiremo nel modo seguente [cfr. Knuth 1965; e Dahlqvist, Björck e Anderson 1974]: un problema computazionale è una descrizione precisa della relazione

funzionale fra i dati d'ingresso – le cosiddette variabili indipendenti del problema – ed i dati di uscita, i risultati desiderati. I dati d'ingresso e quelli di uscita sono rappresentati da vettori (a elementi reali) di dimensione finita. La relazione funzionale può essere espressa tanto in forma implicita quanto in forma esplicita.

Un algoritmo per la risoluzione di un problema computazionale è una descrizione completa di operazioni ben definite che trasformano i dati d'ingresso ammissibili in dati di uscita in un numero finito di passi. Per operazioni ben definite intendiamo operazioni aritmetiche e logiche che, almeno in teoria, possono essere eseguite esattamente e in un tempo finito da una persona che usi soltanto carta e penna. Per un dato problema computazionale si possono considerare diversi algoritmi; essi forniscono in generale risultati con diversi gradi di approssimazione. «Il modo in cui sono trattati dettagli piccoli ma critici negli algoritmi può influenzare la precisione del risultato in maniera che il neofita difficilmente sospetterebbe» [Dahlqvist, Björck e Anderson 1974, p. 138].

La differenza fra algoritmo e problema computazionale può apparire un po' artificiosa: tuttavia «il punto essenziale è che nella formulazione di un problema si considerano solo lo stato iniziale e quello finale. In un algoritmo, invece, si deve chiaramente definire ogni tappa lungo il cammino dall'inizio alla fine» [*ibid.*, p. 14].

Questa caratterizzazione include certamente la vecchia idea dell'algoritmo come «calcolo con decimali» (cfr. § 2.2), ma non si riduce certo a essa.

Ecco alcuni esempi di algoritmi numerici: l'algoritmo euclideo della divisione, che abbiamo supposto noto al lettore, il procedimento euclideo per la ricerca del massimo comun divisore degli interi, il crivello di Eratostene per la determinazione dei numeri primi; ovviamente, la somma ed il prodotto di numeri naturali, interi, relativi, razionali, sono tutti esempi di algoritmi. Non lo è *in sé* la procedura per la radice quadrata di m descritta nel § 3.2; lo diventa però fissando un limite superiore per l'indice n che in essa compare. Il concetto di algoritmo, infine, può essere anche introdotto in problemi di carattere completamente diverso (linguistica matematica, traduzione automatica, ecc.; si veda anche l'articolo «Algoritmo» di questa stessa *Enciclopedia*).

Esaminiamo ora la questione preliminare degli errori connessi con la rappresentazione dei numeri reali su un calcolatore realizzabile praticamente.

Abbiamo visto nel § 3.3 come i numeri reali siano rappresentabili in base n mediante una successione di infinite cifre. Ovviamente tali numeri non possono essere scritti in modo effettivo; si tratta perciò di approssimarli; lo possiamo fare in virgola fissa (in cui si lavora con un numero costante di decimali) oppure in virgola mobile (in cui si lavora con un numero costante di cifre significative).

Limitiamoci ad illustrare quest'ultima approssimazione, sviluppata da Wilkinson intorno al 1960.

Si chiama rappresentazione n-aria in virgola mobile (v. m.) normalizzata del numero reale $a \neq 0$ una rappresentazione della forma $a = f \cdot n^p$ dove $1/n \leq |f| < 1$ e p è un intero relativo. Tale rappresentazione è possibile in modo

unico per ogni numero reale $a \neq 0$. L'intero p è detto esponente e il numero reale f è detto mantissa (o frazione).

In un calcolatore il numero delle cifre per f e per p è limitato: solo un insieme finito di numeri razionali può essere rappresentato in macchina; gli elementi di questo insieme sono detti numeri macchina. Piú precisamente un numero macchina in v. m. (normalizzata) è, per definizione, lo zero oppure un numero razionale avente rappresentazione n-aria $n^p f$ dove p è un intero tale che $-m \leq p \leq M$ e dove f è tale che $f = \pm \sum_{k=1}^{t} a_k n^{-k}$ con t intero ≥ 2, $a_1 \neq 0$ e $0 \leq a_k \leq n-1$ per $k = 2, \ldots, t$; t è detto il numero delle cifre della mantissa. L'insieme di tali numeri macchina verrà indicato $F(n, t, m, M)$ (o solo con F se non ci sono ambiguità); si tratta, ovviamente, di un insieme finito (cfr. fig. 20).

Se scriviamo p nella forma $p = \pm \sum_{k=0}^{l-1} b_k n^k$ con $0 \leq b_k \leq n-1$ allora ogni numero macchina, diverso da zero, può essere rappresentato su calcolatore con la forma schematica illustrata nella figura 21. Un tale numero occupa quindi $l+t+2$ posizioni di memoria. Se invece scriviamo $p = r - s$ dove s è il cosiddetto eccesso, stabilito a priori, e $r = \sum_{k=0}^{l-1} c_k n^k$ con $0 \leq c_k \leq n-1$, si può guadagnare una posizione di memoria.

Osserviamo che ogni numero diverso da zero in v. m. normalizzata verifica la disuguaglianza $n^{-m-1} \leq |n^p f| \leq n^M(1-n^t)$ e l'intervallo $[n^{-m-1}, n^M(1-n^t)]$ è detto rango della variabile in virgola mobile.

Dato un numero reale x vogliamo allora associarvi un numero macchina in v. m. normalizzata che verrà indicato con $\mathrm{fl}(x)$. Naturalmente se $x = 0$ allora $\mathrm{fl}(x) = 0$. Se $x \neq 0$ verifica

$$(1) \qquad n^{-m-1} \leq |x| \leq n^{-M}(1-n^{-t})$$

si può operare in uno dei due modi seguenti:

- troncatura: $\mathrm{fl}(x)$ è l'unico elemento di F che ha distanza minima da x e verifica il vincolo $|\mathrm{fl}(x)| \leq |x|$;
- arrotondamento: $\mathrm{fl}(x)$ è l'elemento di F a distanza minima da x con la convenzione che se vi sono due elementi di F a distanza minima allora si prende quello dei due che è maggiore in valore assoluto.

Se poi $|x|$ non appartiene a $[n^{-m-1}, n^{-M}(1-n^{-t})]$ non vi è possibilità ragionevole di approssimare x con elementi di F; in tale caso si dice che $|x|$ è al di fuori del rango dei numeri in virgola mobile.

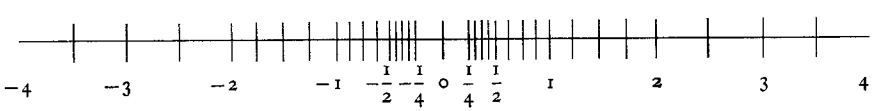


Figura 20.
Rappresentazione dei 33 punti di F per $n=2$, $t=3$, $m=1$, $M=2$.

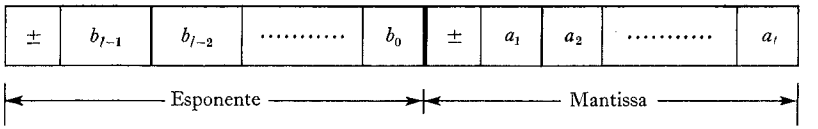


Figura 21.
Rappresentazione schematica di un numero macchina.

Il risultato fondamentale nell'ambito dell'approssimazione in v. m. è fornito dalla seguente maggiorazione dell'errore

$$(2) \qquad \mathrm{fl}(x) = x(1+\delta)$$

con $|\delta| \leq n^{1-t}/2$ (arrotondamento) o $|\delta| \leq n^{1-t}$ (troncatura) valida per ogni x che verifica la (1).

Tenendo conto di ciò è naturale chiamare unità della macchina (o unità di approssimazione) il numero u definito da

$$u = \begin{cases} \dfrac{n^{1-t}}{2} & \text{se è usato l'arrotondamento} \\ n^{1-t} & \text{se è usata la troncatura} \end{cases}$$

tale numero u può essere considerato infatti come unità naturale per le variazioni relative e per gli errori relativi.

L'insieme finito F dei numeri macchina in v. m. non è certamente chiuso rispetto alle quattro operazioni dell'aritmetica (per esempio il prodotto di due numeri x, y in v. m. con t cifre di mantissa è un numero razionale rappresentato in v. m. con $2t$ oppure $2t-1$ cifre di mantissa). A tale inconveniente si può ovviare approssimando il risultato con un numero in virgola mobile che noi indicheremo con $\mathrm{fl}(x+y)$, $\mathrm{fl}(x-y)$, $\mathrm{fl}(x \cdot y)$, $\mathrm{fl}(x/y)$.

Un problema naturale è quello di valutare gli errori che si commettono eseguendo le pseudo-operazioni cosí definite, errori che dipendono dalla struttura interna (*hardware*) del calcolatore: in generale, qualora il risultato verifichi la (1), esso viene approssimato per troncatura od arrotondamento; se invece il risultato non verifica la (1), allora l'elaboratore segnala il tipo di errore commesso, detto di *overflow*, rispettivamente di *underflow*, se l'esponente diventa troppo grande, rispettivamente troppo piccolo.

Se il risultato dell'operazione verifica la (1), si dànno le seguenti valutazioni dell'errore con $|\delta| \leq u$:

$$(3) \qquad \begin{aligned} \mathrm{fl}(x \pm y) &= (x \pm y)(1+\delta) \\ \mathrm{fl}(xy) &= xy(1+\delta) \\ \mathrm{fl}\left(\frac{x}{y}\right) &= \frac{x}{y}(1+\delta) \end{aligned}$$

È importante sottolineare come le pseudo-operazioni cosí definite non verificano tutti gli assiomi del § 2 [uno studio assai accurato delle regole delle pseudo-operazioni si trova in Knuth 1969, cap. IV].

Per esempio l'associatività non vale per la pseudo-operazione somma. Si considerino infatti i numeri in base 10 con 7 cifre di mantissa: $a = 0{,}3234521 \cdot 10^0$, $b = 0{,}4859312 \cdot 10^4$, $c = -b$.

Risulta allora $\mathrm{fl}(b+c) = 0$ e quindi $\mathrm{fl}(a+\mathrm{fl}(b+c)) = a$. Peraltro $a+b = 0{,}48596354521 \cdot 10^4$, e quindi $\mathrm{fl}(a+b) = 0{,}4859635 \cdot 10^4$, da cui $\mathrm{fl}(a+b)+c = 0{,}0000323 \cdot 10^4$, e infine $\mathrm{fl}(\mathrm{fl}(a+b)+c) = 0{,}3230000 \cdot 10^0 \neq \mathrm{fl}(a+\mathrm{fl}(b+c))$.

L'esempio mostra come due algoritmi possano essere equivalenti dal punto di vista matematico (se eseguiti cioè con infinite cifre decimali) ma possano dare risultati numerici diversi.

«Il calcolo in virgola mobile è per natura inesatto e non è difficile usarlo cosí male che le risposte calcolate consistono quasi esclusivamente di "rumore" [*noise*]. Uno dei problemi principali dell'analisi numerica è quello di determinare quanto siano accurati i risultati di un certo metodo numerico; si tratta di un problema di *credibility gap*: non sappiamo quanto credere alle risposte del calcolatore. Chi usa il calcolatore per le prime volte risolve la questione avendo fede nel calcolatore come in una autorità infallibile; tende a credere che tutte le cifre di una risposta stampata siano significative. Chi usa il calcolatore da molto tempo ha proprio l'attitudine opposta: teme costantemente che le risposte siano quasi senza senso» [Knuth 1969, p. 195].

Le formule (3) possono essere interpretate dicendo che il risultato di una pseudo-operazione su x e y coincide con il risultato di una operazione esatta su x ed $y(1+\delta)$ e cioè con il risultato di un'operazione esatta in cui l'operando è stato perturbato con un errore relativo inferiore ad u. L'analisi retrograda dell'errore di un algoritmo applica tale interpretazione a ogni tappa dell'algoritmo. Si può in tal modo dimostrare che il risultato ottenuto mediante l'algoritmo (tenendo conto degli errori di arrotondamento o troncatura) è il risultato esatto di un problema dello stesso tipo nel quale i dati d'ingresso sono stati perturbati di poche unità u. La misura di tale cambiamento viene detta *condizionamento* dell'algoritmo; ovviamente quanto piú essa è piccola tanto piú l'algoritmo è efficiente o, come si suol dire, ben condizionato.

In modo analogo si dice condizionamento di un problema computazionale il massimo errore relativo a cui possono essere soggetti i risultati in seguito ad un errore relativo nei dati d'ingresso.

Quest'ottica ci permette di raffinare ulteriormente i requisiti esposti nel § 3.8 circa i problemi ben posti: le tre condizioni di esistenza, unicità e di dipendenza continua dei dati fanno propria, in certo qual modo, l'esigenza «positivista» di trattare solo questioni «significanti»: ma ciò non basta ancora. I problemi possono infatti essere ben posti, ma mal condizionati (si vedano per esempio nel § 4.4 i casi tratti dall'analisi numerica lineare o nel § 4.8 quanto detto per le equazioni differenziali ordinarie).

La ragione principale di tale fatto si ritrova nella dicotomia continuo/discreto: nella definizione di funzione continua in x_0 data nel § 3.3 – la classica

definizione ε-δ di Weierstrass – a ogni $\varepsilon > 0$ piccolo a piacere corrisponde almeno un $\delta > 0$; ma nei problemi numerici non possiamo piú prendere ε arbitrario: per esempio non possiamo prendere ε al di sotto della soglia dell'*underflow*, cioè di n^{-m-1}.

4.4. Algebra lineare numerica.

Gli operatori lineari s'incontrano comunemente nello sviluppo di argomenti sia teorici sia applicativi (basti pensare per esempio che la derivata e l'integrale sono operatori lineari, che i problemi ben posti considerati nel § 3.8 si interpretano come operatori lineari, ecc.). Un operatore lineare in $\mathbf{R}^n$ è rappresentato da una matrice quadrata e quindi risolvere il sistema di equazioni lineari

$$(4) \qquad \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \cdots\cdots\cdots\cdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n \end{cases}$$

significa: dato $b \in \mathbf{R}^n$ trovare $x \in \mathbf{R}^n$ tale che $Ax = b$ dove A è l'operatore associato alla matrice $(a_{ij})_{i,j=1,\ldots,n}$.

È stato valutato che la soluzione di un sistema di equazioni interviene in un modo o nell'altro nella risoluzione di tre problemi scientifici su quattro; è quindi cruciale avere un modo efficiente per risolvere tali sistemi.

«L'algebra lineare è una buona illustrazione della differenza tra matematica classica ed analisi numerica. Anche se la teoria era nota da secoli, i passi decisivi nel trattamento numerico del problema [(4)]... sono stati fatti per la prima volta negli ultimi decenni. Le *formule esplicite coi determinanti* per la matrice inversa e per la soluzione di un sistema di equazioni lineari (regola di Cramer) sono *assolutamente antieconomiche* nei calcoli numerici tranne che per matrici 2×2 o 3×3 o eventualmente per matrici con struttura molto particolare» [Dahlqvist, Björck e Anderson 1974, pp. 137-38].

Supponiamo che (4) sia ben posto: a tal fine è necessario e sufficiente che $\det A \neq 0$ poiché allora la soluzione esiste ed è unica comunque sia dato $b \in \mathbf{R}^n$; inoltre $A^{-1} : \mathbf{R}^n \to \mathbf{R}^n$ è un operatore lineare e continuo per ogni norma ragionevole su $\mathbf{R}^n$ (per esempio la norma euclidea $\|x\|_2 = \left(\sum_{i=1}^{n} x_i^2\right)^{1/2}$ oppure la norma del massimo $\|x\|_\infty = \max_{1 \le i \le n} |x_i|$; indicheremo con $|||A|||_2$ risp. $|||A|||_\infty$ la corrispondente norma per la matrice A).

Se $\det A \neq 0$ la soluzione di (4) è in astratto $x = A^{-1}b$; ma il problema concreto è quello di calcolare tale soluzione: basti pensare che nella pratica si possono incontrare sistemi di equazioni con n dell'ordine di 50 000 o anche 100 000 (in tali casi già il problema della memorizzazione dei coefficienti e l'organizzazione dei dati in ingresso ed in uscita pongono seri problemi: cfr. anche il § 6).

Per risolvere il sistema (4) sono stati studiati diversi metodi che possono dividersi in due categorie:

- metodi diretti: la soluzione è ottenuta – a meno degli errori dovuti alle pseudo-operazioni – in un numero finito di passi;
- metodi iterativi: la soluzione è il limite di una successione di vettori.

Poiché nel § 4.5 esamineremo i procedimenti iterativi per risolvere equazioni non-lineari, ci limitiamo qui a illustrare brevemente il piú famoso dei metodi diretti: il metodo di eliminazione di Gauss in cui a ogni tappa viene eliminata una incognita nel modo seguente.

Supponiamo $a_{11} \neq 0$. Si può allora eliminare x_1 dalle ultime $(n-1)$ equazioni sottraendo dalla i-esima equazione la prima equazione moltiplicata per

$$(5) \qquad m_{i1} = \frac{a_{i1}}{a_{11}} \qquad i = 2, \ldots, n.$$

Il sistema (4) si trasforma allora nel sistema equivalente

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \ldots + a_{1n}x_n = b_1 \\ \qquad a_{22}^{(2)}x_2 + a_{23}^{(2)}x_3 + \ldots + a_{2n}^{(2)}x_n = b_2^{(2)} \\ \qquad a_{32}^{(2)}x_2 + a_{33}^{(2)}x_3 + \ldots + a_{3n}^{(2)}x_n = b_3^{(2)} \\ \qquad \cdots\cdots\cdots\cdots \\ \qquad a_{n2}^{(2)}x_2 + a_{n3}^{(2)}x_3 + \ldots + a_{nn}^{(2)}x_n = b_n^{(2)} \end{cases}$$

dove i nuovi coefficienti sono dati da

$$(6) \qquad \begin{aligned} a_{ij}^{(2)} &= a_{ij} - m_{i1}a_{ij} \\ b_i^{(2)} &= b_i - m_{i1}b_1 \end{aligned} \qquad i, j = 2, \ldots, n.$$

Supponiamo $a_{22}^{(2)} \neq 0$. Si può allora eliminare x_2 dalle ultime $(n-2)$ equazioni sottraendo dalla i-esima equazione la seconda moltiplicata per

$$(7) \qquad m_{i2} = \frac{a_{i2}^{(2)}}{a_{22}^{(2)}} \qquad i = 2, \ldots, n.$$

Il sistema equivalente che si ottiene è il seguente:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \ldots + a_{1n}x_n = b_1 \\ \qquad a_{22}^{(2)}x_2 + a_{23}^{(2)}x_3 + \ldots + a_{2n}^{(2)}x_n = b_2^{(2)} \\ \qquad\qquad a_{33}^{(3)}x_3 + \ldots + a_{3n}^{(3)}x_n = b_3^{(3)} \\ \qquad\qquad \cdots\cdots\cdots\cdots \\ \qquad\qquad a_{n3}^{(3)}x_3 + \ldots + a_{nn}^{(3)}x_n = b_n^{(3)} \end{cases}$$

dove

$$(8) \qquad \begin{aligned} a_{ij}^{(3)} &= a_{ij}^{(2)} - m_{i2}a_{2j}^{(2)} \\ b_i^{(3)} &= b_i^{(2)} - m_{i2}b_2^{(2)} \end{aligned} \qquad i, j = 3, \ldots, n.$$

Se $a_{33}^{(3)} \neq 0$ si può eliminare x_3 e cosí via; otteniamo infine:

$$(9) \qquad \begin{cases} a_{11}^{(1)}x_1 + a_{12}^{(1)}x_1 + a_{13}^{(1)}x_3 + \ldots + a_{1n}^{(1)}x_n = b_1^{(1)} \\ \qquad a_{22}^{(2)}x_1 + a_{23}^{(2)}x_3 + \ldots + a_{2n}^{(2)}x_n = b_2^{(2)} \\ \qquad\qquad a_{33}^{(3)}x_3 + \ldots + a_{3n}^{(3)}x_n = b_3^{(3)} \\ \qquad\qquad \cdots\cdots\cdots\cdots \\ \qquad\qquad\qquad a_{nn}^{(n)}x_n = b_n^{(n)} \end{cases}$$

dove per comodità abbiamo introdotto la notazione $a_{1j}^{(1)} = a_{1j}$, $b_1^{(1)} = b_1$ per i coefficienti ed il termine noto del sistema originale.

Gli elementi $a_{11}^{(1)}$, $a_{22}^{(2)}$, $a_{33}^{(3)}$, ... che abbiamo supposto $\neq 0$ sono detti i pivot del metodo ed essi risultano certamente $\neq 0$ pur di fare una eventuale permutazione delle righe (a causa dell'ipotesi $\det A \neq 0$). Converrà anzi scegliere i pivot in modo che $|m_{ik}| \leq 1$ per ogni i, k.

Il sistema triangolare (9) può essere poi facilmente risolto con le cosiddette formule di sostituzione all'indietro ottenendo

$$(10) \qquad \begin{cases} x_n = \dfrac{b_n^{(n)}}{a_{nn}^{(n)}} \\ x_{n-1} = \dfrac{b_{n-1}^{(n-1)} - a_{n-1,n}^{(n-1)}x_n}{a_{n-1,n-1}^{(n-1)}} \\ \cdots\cdots\cdots\cdots \\ x_1 = \dfrac{b_1^{(1)} - a_{n1}^{(1)}x_n - \ldots - a_{n2}^{(1)}x_2}{a_{11}^{(1)}}. \end{cases}$$

Dal punto di vista del numero totale delle operazioni è agevole verificare che per ottenere il sistema (9) si devono effettuare in generale $n(n-1)/2$ divisioni, $(n^3-n)/3$ addizioni e lo stesso numero di moltiplicazioni. La risoluzione del sistema (9) richiede poi n divisioni e $n(n-1)/2$ addizioni e altrettante moltiplicazioni. In totale dunque il numero di addizioni e di moltiplicazioni è $(n^3/3) + O(n^2)$ per n tendente all'infinito. Il metodo di Gauss è dunque incomparabilmente piú veloce della regola di Cramer per la quale necessitano $O(n!)$ operazioni.

Osserviamo subito che il numero di operazioni può essere sostanzialmente ridotto nel caso di matrici sparse (e cioè con molti elementi $=0$) tenendo opportunamente conto della presenza degli elementi certamente nulli. Per il problema generale di quale sia il numero minimo di operazioni teoricamente necessario nel caso di una matrice qualunque si veda il § 6.2.

Alla luce di quanto detto nel § 4.3 esaminiamo ora la questione del condizionamento del sistema (4). Si tratta allora di confrontare la soluzione dei due sistemi $Ax = b$ ed $A(x + \delta x) = b + \delta b$, e cioè l'influenza di una perturbazione del dato d'ingresso b. In tale caso si ottiene

$$\frac{\|\delta x\|}{\|x\|} \leq \mu(A) \frac{\|\delta f\|}{\|f\|}$$

dove $\mu(A) = |||A||| \,/\, |||A^{-1}||| \geq 1$ è detto il condizionamento di A ($\|x\|$ è una qualunque norma su $\mathbf{R}^n$ e $|||A|||$ la corrispondente norma per la matrice e cioè $|||A||| = \sup_{x \neq 0} \|Ax\| \,/\, \|x\|$; cfr. § 3.8).

Si consideri ad esempio la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1{,}00001 \end{pmatrix}$$

allora $\mu(A)$ è circa 10^5 e quindi il problema è mal condizionato, infatti assumendo $b = \begin{pmatrix} 2 \\ 2{,}00001 \end{pmatrix}$ la soluzione è $x_1 = x_2 = 1$ mentre assumendo $b = \begin{pmatrix} 2 \\ 1{,}9999 \end{pmatrix}$ la soluzione è $x_1 = 12$, $x_2 = -10$.

La prima analisi completa degli errori (di arrotondamento o troncatura) del metodo di Gauss è stata fatta da Wilkinson (1960). Illustriamo brevemente tale analisi seguendo l'esposizione fattane da Forsythe e Moler [1967]. Supponiamo innanzitutto che $a_{kk}^{(k)} \neq 0$ per ogni $k = 1, \ldots, n$, cosa come si è visto sempre possibile a meno di una permutazione di righe.

L'algoritmo corrispondente al metodo di Gauss consiste nel calcolare una successione di matrici $A^{(1)} = A, \bar{A}^{(2)}, \ldots, \bar{A}^{(n)}$ dove la matrice $\bar{A}^{(k)}$ ha elementi tutti nulli sotto la diagonale delle prime $k-1$ colonne. La matrice $\bar{A}^{(k+1)}$ è poi ottenuta dalla matrice $\bar{A}^{(k)}$ sottraendo un multiplo della k-esima riga da ogni rigo sotto la k-esima; il resto di $\bar{A}^{(k)}$ non essendo modificato. I moltiplicatori sono scelti in modo che se non ci fossero errori di arrotondamento (o troncatura) nella matrice $\bar{A}^{(k+1)}$ tutti gli elementi sotto la diagonale della k-esima riga sarebbero nulli. Noi non li calcoliamo: li assumiamo nulli per definizione.

In modo piú preciso indichiamo con $\bar{a}_{ij}^{(k)}$ gli elementi della matrice $\bar{A}^{(k)}$, allora risulta (cfr. le formule 5-8)

$$\bar{m}_{ik} = \mathrm{fl}\frac{\bar{a}_{ik}^{(k)}}{\bar{a}_{kk}^{(k)}} \qquad i = k+1, \ldots, n$$

$$\bar{a}_{ij}^{(k+1)} = \begin{cases} 0 & \text{per } k+1 \leq i \leq n \text{ e } j = k \\ \mathrm{fl}(\bar{a}_{ij}^{(k)} - \bar{m}_{ik}\bar{a}_{kj}^{(k)}) & \text{per } k+1 \leq i,\ j \leq n \\ \bar{a}_{ij}^{(k)} & \text{altrimenti.} \end{cases}$$

Tenendo conto delle formule (3) si prova che la soluzione calcolata $x + \delta x$ può essere considerata come la soluzione esatta del problema perturbato $(A + \delta A)(x + \delta x) = b$ ove la perturbazione δA dipende in generale da b.

Nell'ipotesi $|||\delta A||| < 1 / |||A^{-1}|||$ si dimostra la maggiorazione

$$\frac{\|\delta x\|}{\|x\|} \leq \frac{\mu(A)}{1 - |||\delta A||| \; |||A^{-1}|||} \; \frac{|||\delta A|||}{|||A|||}$$

e quindi il problema è ricondotto a valutare $|||\delta A|||$. È questa la parte piú delicata del lavoro di Wilkinson in quanto tale maggiorazione dipende dalla

«strategia pivotale» e cioè dalla scelta dei pivot. Se i pivot sono scelti in modo che $|\bar{m}_{ik}| \leq 1$ per ogni i, k allora nell'ipotesi che sia $nu \leq 0{,}01$ (ove u è l'unità di approssimazione della macchina; cfr. p. 457) si ottiene la maggiorazione

$$(11) \qquad |||\delta A|||_\infty \leq 1{,}01(n^3 + 3n^2)\rho |||A|||_\infty u$$

dove $\rho = \max_{i,j,k} |\bar{a}_{ij}^{(k)}| / |||A|||_\infty$, quantità che può essere facilmente calcolata durante l'esecuzione dell'algoritmo. Si osservi che, pur dipendendo δA da b, la maggiorazione (11) risulta indipendente da b. Inoltre tale maggiorazione è certamente pessimistica: «Noi non conosciamo alcun esempio in cui $|||\delta A|||_\infty$ anche solo si avvicini alla maggiorazione trovata» [Forsythe e Moler 1967, p. 107].

Argomento di studio è naturalmente la determinazione a priori di quanto possano crescere i coefficienti $|\bar{a}_{ij}^{(k)}|$ durante il processo di eliminazione di Gauss, per esempio quando $|a_{ij}| \leq 1$ per ogni $i, j = 1, \ldots, n$. Wilkinson (1967) ha provato che, usando la strategia del pivot parziale per righe, per cui $|\bar{m}_{ik}| \leq 1$ per ogni i, k, si ha la maggiorazione (catastrofica!: cfr. la tabella nel § 3.4)

$$g(n) = \frac{\max_{i,j,k} |\bar{a}_{ij}^{(k)}|}{\max_{i,j} |a_{ij}|} \leq 2^{n-1}$$

e che esistono matrici, invero assai speciali, per cui tale limitazione è raggiunta. Se si usa la piú complicata strategia del pivot totale per cui il pivot è l'elemento piú grande in valore assoluto dell'intera matrice delle equazioni che rimangono, allora Wilkinson ha provato che si ha $g(n) \leq 1{,}8 n^{0{,}25 \log n}$.

La maggiorazione per $g(n)$ con pivot totale è molto minore per grandi valori di n, e giustificherebbe il maggior lavoro necessario. Il guadagno è, tuttavia, piú che altro teorico giacché l'esperienza pratica mostra che assai raramente $g(n)$ supera 8 anche con la strategia del pivot parziale! [Dahlqvist, Björck e Anderson 1974, p. 180].

4.5. Processi iterativi.

Le radici di una equazione non-lineare $f(x) = 0$ non possono in generale scriversi in modo esplicito e quand'anche ciò è possibile l'espressione è spesso di nessuna pratica utilità. Per risolvere le equazioni non-lineari si devono dunque utilizzare dei metodi approssimati iterativi e cioè tali che partendo da uno o piú punti iniziali essi definiscono una successione $x_0, x_1, x_2, \ldots$ di numeri che si spera convenga alla soluzione voluta. Tali metodi iterativi sono essenzialmente basati su due possibilità: approssimazioni successive, oppure linearizzazione. Illustreremo ora alcuni metodi che rientrano nell'una o nell'altra categoria per la determinazione di una radice ξ_0 dell'equazione $f(x) = 0$.

Ricordiamo preliminarmente la definizione di ordine di convergenza della

successione x_n a ξ_0. Supponiamo a tal fine che sia $\lim_{n\to\infty} x_n = \xi_0$ e poniamo $\varepsilon_n = x_n - \xi_0$. Se esistono un numero p ed una costante $C \neq 0$ tali che

$$\lim_{n\to\infty} \frac{|\varepsilon_{n+1}|}{|\varepsilon_n|^p} = C$$

allora p è detto ordine di convergenza della successione. Per $p = 1, 2, 3$ la convergenza è detta lineare, quadratica e cubica rispettivamente.

Ricordiamo poi che il confronto fra metodi iterativi per approssimare ξ_0 è fatto non solo in termini di ordine di convergenza ma anche di quantità di calcoli richiesti ad ogni iterazione (essenzialmente il numero di volte in cui si deve calcolare $f(x)$ o le sue derivate): si tratta di un esempio di problema di complessità computazionale (cfr. § 6).

Relativamente all'influenza degli errori di arrotondamento (o troncatura) osserviamo subito che in generale non si raggiungerà la soluzione esatta, ma ci si fermerà a una soluzione approssimata ξ^* che a priori non si conosce quanto possa distare dalla soluzione esatta. Tuttavia si può valutare l'accuratezza raggiungibile per la soluzione esatta ξ_0 nel modo seguente. Quando ξ_0 è radice semplice, e cioè $f'(\xi_0) \neq 0$, dal teorema del valor medio si ha $f(x_n) = (x_n - \xi_0) f'(\alpha)$ dove $\alpha \in \mathcal{J}$ intervallo di estremi ξ_0 ed x_n, e quindi

$$|x_n - \xi_0| \leq \frac{|f(x_n)|}{M_1}$$

ove $M_1 \geq |f'(x)|$ per $x \in \mathcal{J}$. Il valore calcolato $f(\bar{x}_n)$ di $f(x_n)$ verifica in generale $f(\bar{x}_n) = f(x_n) + \delta(x_n)$ ove $|\delta(x_n)| \leq \delta$ indipendente da x; l'accuratezza con cui ξ_0 può essere valutato dipende da δ; ed al meglio si può avere $f(x_n) = 0$ e quindi $|f(\bar{x}_n)| \leq \delta$. Supponendo che $f'(x)$ non vari molto vicino a ξ_0 si ottiene in conclusione

$$|\bar{x}_n - \xi_0| \leq \frac{\delta}{M_1}$$

ove δ/M_1 ha circa il valore di $\varepsilon_{\xi_0} = \delta/f'(\xi_0)$, e dunque la migliore maggiorazione dell'errore, qualunque sia il metodo usato, è ε_{ξ_0}.

Se la radice ξ_0 ha molteplicità p per cui $f'(\xi_0) = \ldots = f^{(p-1)}(\xi_0) = 0$ e $f^{(p)}(\xi_0) \neq 0$ si ha in modo analogo

$$\varepsilon_{\xi_0} = \left(\frac{\delta p!}{|f^{(p)}(\xi_0)|} \right)^{1/p}.$$

Appare chiaro che il problema del calcolo di ξ_0 sarà tanto peggio condizionato quanto piú $f^{(p)}(\xi_0)$ è piccolo (cfr. fig. 22).

1. *Regula falsi.* Supponiamo che f sia definita e continua nell'intervallo chiuso $[a, b]$ e che $f(a)f(b) < 0$; una proprietà fondamentale delle funzioni continue (cfr. § 3.3) assicura che allora esiste almeno un $\xi_0 \in [a, b]$ tale che $f(\xi_0) = 0$ (fig. 23).

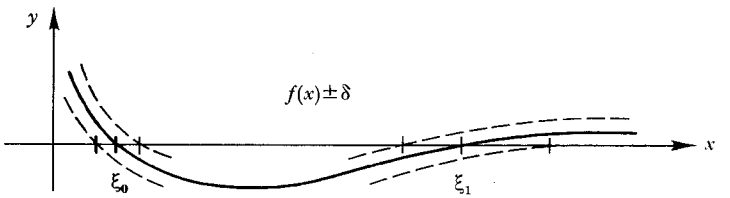


Figura 22.
ξ_0 è ben condizionato, ξ_1 è mal condizionato.

L'idea è allora quella di sostituire a f un polinomio di primo grado $L(x)$ che prende gli stessi valori di f negli estremi a e b. Orbene, per l'ipotesi fatta L si annulla in un punto ξ_1 di $[a, b]$ che si prende come valore approssimativo di ξ_0. Si tratta cioè di un processo di linearizzazione di f.

Il procedimento viene iterato prendendo l'intervallo $[a, \xi_1]$ o quello $[\xi_1, b]$ in cui f assume valori di segno diverso agli estremi.

In modo piú formale, dati i valori iniziali $x_0 = a$ ed $x_1 = b$ si definisce per induzione la successione

$$x_{n+1} = x_n - f(x_n) \frac{x_n - x_{n'}}{f(x_n) - f(x_{n'})}$$

ove n' è il piú grande intero minore n tale che $f(x_n) \cdot f(x_{n'}) < 0$.

Il vantaggio della *regula falsi* è che essa risulta sempre convergente, ma la sua convergenza è solo lineare (come si vede per esempio nel caso di una funzione convessa).

2. *Metodo di Newton-Raphson.* L'idea di fondo di questo metodo è molto simile a quella della *regula falsi*, ma, invece di prendere per L il polinomio tale che $L(x) = y$ risulti l'equazione di una secante alla curva $y = f(x)$ (cfr. fig. 23), tale polinomio si prende in modo che $L(x) = y$ sia l'equazione di una parallela a una tangente di tale curva. Si pone cioè

$$L(x) = f'(z)(x - x_0) + f(x_0).$$

Anche questo procedimento di linearizzazione può venir iterato e permette di stabilire l'esistenza e l'unicità della radice ξ_0 dell'equazione $f(x) = 0$ nell'intervallo $[x_0 - c, x_0 + c]$; per esempio quando esiste $\lambda > 0$ tale che $|f(x_0)| \leq c/2\lambda$ e inoltre tale che quali che siano i punti x, y in $[x_0 - c, x_0 + c]$, si ha $|f'(x)| \geq 1/\lambda$ e $|f'(x) - f'(y)| \leq 1/2\,\lambda$. Sotto tale ipotesi se (z_n) è una successione qualsiasi di punti di $[x_0 - c, x_0 + c]$ si può definire una successione (x_n) di punti di questo intervallo con la formula iterativa

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(z_n)}$$

e tale successione tende a ξ_0.

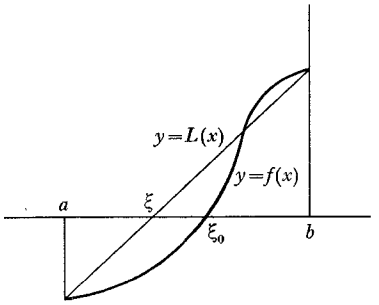


Figura 23.
Regula falsi.

Il metodo di Newton-Raphson ha convergenza quadratica ed è quindi di grande interesse pratico; tuttavia, come si è visto, converge solo partendo abbastanza vicini alla soluzione ξ_0.

3. *Metodi di approssimazione successiva.* La *regula falsi* ed il metodo di Newton-Raphson possono essere considerati come casi particolari del metodo generale di approssimazione successiva, che consiste nel determinare x_{n+1} come funzione di f e delle sue derivate negli m punti $x_n, x_{n-1}, \ldots, x_{n-m+1}$: $x_{n+1}=g(x_n, \ldots, x_{n-m+1})$.

La funzione g è detta funzione di iterazione a m punti. Nel caso particolare in cui $m=1$ la convergenza del metodo significa intuitivamente determinare un punto fisso di g e cioè un punto ξ_0 tale che

$$\xi_0=g(\xi_0). \tag{12}$$

Tale punto fisso è poi soluzione di $f(x)=0$ se si assume per esempio $g(x)=x-f(x)$.

La determinazione di un punto fisso è uno strumento generale dell'analisi non-lineare anche per provare l'esistenza della soluzione di una equazione (e non solamente per approssimarla) come si è visto col procedimento di Peano-Picard nel § 3.7. Nel caso di g, applicazione di uno spazio di Banach in sé, la teoria dei punti fissi è strettamente collegata con profonde considerazioni di topologia (teoria del grado topologico, teoremi di Brouwer, Leray-Schauder, ecc.).

Relativamente alla ricerca di un punto fisso per (12) ricordiamo il seguente teorema: se x_0 è un punto di $I=[a, b]$ e supponiamo che esista un intervallo (x_0-c, x_0+c) incluso in I e un numero q tale che $0<q<1$ con le proprietà $|g(x_1)-g(x_2)|\leq q|x_1-x_2|$ per ogni coppia x_1, x_2 di (x_0-c, x_0+c) e $|g(x_0)-x_0|\leq c(1-q)$; allora esiste una e una sola soluzione $\xi_0\in(x_0-c, x_0+c)$ della equazione (12) e si può inoltre definire per induzione una successione (x_n) ponendo $x_{n+1}=g(x_n)$ per $n\geq 0$ per cui vale $|\xi_0-x_n|\leq cq^n$ onde (x_n) converge a ξ_0 (cfr. fig. 24).

Sottolineiamo per concludere che il metodo delle approssimazioni successive costituisce un modo notevolmente suggestivo di risolvere la dicotomia dimostra-

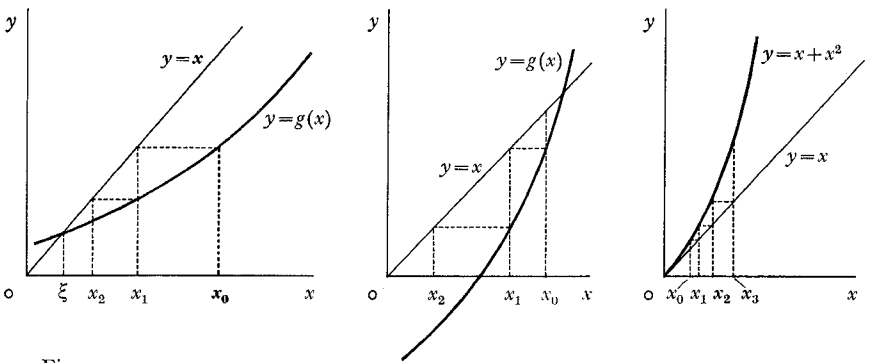


Figura 24.

Metodo delle iterazioni successive. Servendoci del grafico della funzione g possiamo facilmente rappresentare la costruzione delle approssimazioni x_n alla soluzione ξ_0 del problema. Da tale rappresentazione si vede che il metodo non dà piú una successione convergente a ξ_0 se si abbandona la restrizione che la derivata di g' di g sia in valore assoluto minore di 1. Per rendersene conto basta prendere $g(x)=x+x^2$ e $x_0>0$ per avere una successione (x_n) che tende a $+\infty$.

zioni di esistenza / procedure di approssimazione, giacché il teorema precedente si estende facilmente al caso degli spazi di Banach.

4.6. Approssimazione di funzioni.

«Un problema fondamentale che si presenta in molte varianti, è approssimare una funzione f mediante un elemento f^* di una classe di funzioni facili da trattare matematicamente (per esempio, polinomi, funzioni razionali o polinomi trigonometrici) dove ogni funzione particolare della classe è determinata dai valori numerici di un certo numero di parametri... Vi sono due tipi di imperfezione da prendere in considerazione: imperfezioni nei dati d'ingresso e imperfezioni nel modello particolare (classe o forma delle funzioni) che si vuole adattare ai dati d'ingresso. Per semplicità chiameremo tali imperfezioni *errore di misura* e rispettivamente *errore del modello*... In pratica sia i dati d'ingresso sia il modello sono in generale insufficienti. Si può considerare l'approssimazione come caso speciale di un problema piú generale e veramente importante: adattare un *modello* matematico ai dati assegnati ed altri fatti noti. I problemi di approssimazione possono essere considerati analoghi a quelli dell'ingegneria delle comunicazioni: filtrare il *segnale* dal *rumore*» [Dahlqvist, Björck e Anderson 1974, pp. 81, 83].

1. *Interpolazione di Lagrange.* È noto che due punti distinti individuano una retta, tre punti una parabola (con asse parallelo all'asse y), ecc. Congetturiamo allora che esista e sia unico un polinomio di grado n, la curva del quale

passa per $n+1$ punti prefissati. La teoria astratta conferma agevolmente la nostra congettura: dati gli $n+1$ punti distinti x_i, $i=0, 1, \ldots, n$ e i corrispondenti valori $f(x_i)=y_i$, si tratta di «trovare» i coefficienti $a_0, a_1, \ldots, a_n$ del cosiddetto polinomio di interpolazione $P_n(x)=a_0x^n+\ldots+a_n$ in modo tale da minimizzare l'errore

$$(13) \qquad \sum_{i=0}^{n} |f(x_i)-P_n(x_i)|$$

cioè la somma degli scarti (in valore assoluto) tra P_n e f nei nodi x_i. Se imponiamo che l'errore (13) sia nullo è

$$(14) \qquad P_n(x_i)=f(x_i) \qquad i=0, 1, \ldots, n$$

per gli n nodi x_i e il nostro problema diventa quello di determinare i coefficienti $a_0, \ldots, a_n$ intesi come le $n+1$ incognite del sistema (14) di $n+1$ equazioni lineari. È un problema classico di algebra lineare: perché (14) ammetta una e una sola soluzione, è necessario e sufficiente che il sistema di equazioni omogenee corrispondente $P_n(x_i)=0$ ammetta solo la soluzione banale $a_0=a_1=\ldots=a_n=0$. Questo è proprio il nostro caso, dato che il sistema omogeneo impone al polinomio $P_n(x)$ di grado al piú n di annullarsi in $n+1$ punti distinti $x_0, x_1, \ldots, x_n$ e in questo modo si impone al polinomio una radice zero di troppo.

Sfruttando cosí una classica proprietà dei polinomi che li privilegia rispetto a funzioni di diverso tipo (il numero delle radici distinte di un polinomio non nullo non supera il suo grado), possiamo dare risposta affermativa al nostro quesito. Ma per n «abbastanza» grande i metodi algebrici «classici» sono di fatto inutilizzabili per determinare la soluzione del problema. La nostra risposta affermativa valeva dunque quanto una pura dimostrazione di esistenza. Tuttavia queste considerazioni teoriche non sono sterili: esse garantiscono la correttezza grammaticale della locuzione 'il' quando esprimiamo *il* polinomio di interpolazione per altra via.

Possiamo per esempio procedere in questo modo. Introduciamo i polinomi interpolatori di Lagrange

$$\omega_n(x)=(x-x_0)(x-x_1)\ldots(x-x_n) \qquad \text{per } i=0, 1, \ldots, n$$

e posto $\omega'_n(x_i)=(d\omega_n x/dx)_{x=x_i}$ definiamo per $i=0, 1, \ldots, n$

$$q_{n,i}(x)=\frac{\omega_n(x)}{(x-x_i)\,\omega'_n(x_i)}$$

e otteniamo allora

$$P_n(x)=\sum_{i=0}^{n} f(x_i)\, q_{n,i}(x).$$

Questa strategia – usualmente nota come interpolazione di Lagrange – comporta ovviamente un errore puntuale

$$R_n(x)=f(x)-P_n(x)$$

per x che varia nell'intervallo base $I=[a, b]$. Due sono i nostri obiettivi: darne un'espressione esplicita e stimarlo, cioè maggiorarlo e minorarlo. Si dimostra che per ogni punto x di $[a, b]$ esiste un punto $\xi=\xi(x)$ dipendente da x nell'intervallo aperto (a, b) tale che

$$\min(x_0, x_1, \ldots, x_n, x)<\xi<\max(x_0, x_1, \ldots, x_n, x)$$

tale che l'errore $R_n(x)$ risulta uguale a

$$(15) \qquad \frac{\omega_n(x)}{(n+1)!}\, f^{(n+1)}(\xi)$$

ove al solito abbiamo indicato con $f^{(n+1)}$ la derivata $n+1$-esima di f. Di questo teorema «classico» vediamo l'uso «costruttivo» se riusciamo a determinare nell'intervallo $[a, b]$ il massimo e il minimo di $f^{(n+1)}(x)$; la formula (15) ci permette di stimare l'errore.

Tale stima dipende dunque dalla nostra conoscenza dei massimi e minimi di $f^{(n+1)}(x)$. Siamo qui al nocciolo della questione. Ovviamente il polinomio $P_n(x)$ è compatibile con tutte le funzioni di una certa classe che assumono i valori y_i nei nodi x_i; ma appunto sotto il profilo predittivo risulta essenziale chiedersi sotto quali condizioni l'errore puntuale d'interpolazione converge a 0 al crescere dei nodi, cioè con l'aumento della nostra informazione. La speranza di un teorema ottimale è presto delusa: se per $f(x)$ prendiamo $x \sin \pi/x$ nei nodi $x_n=1/n$ i polinomi di interpolazione risultano tutti identicamente nulli e quindi in generale non convergono alla funzione interpolata. Possiamo però rendere «piú esigenti» le condizioni che imponiamo su f. Cosí, se la funzione f è *analitica*, la successione dei polinomi di Taylor (che possono essere considerati come polinomi di interpolazione in cui $x_0=x_1=\ldots=x_n$) converge a f in un intervallo $\mathcal{J}$. Questo intervallo è però il diametro del massimo cerchio nel quale f si può prolungare in modo olomorfo: di conseguenza l'intervallo (reale) $\mathcal{J}$ di convergenza può essere notevolmente minore dell'intervallo base I: $1/(1+x^2)$ è analitica per ogni x reale, mentre l'intervallo $\mathcal{J}$ di convergenza dei polinomi d'interpolazione con l'unico nodo 0 è l'intervallo aperto $(-1, +1)$. Ci chiediamo allora se si può rimuovere questa limitazione interpolando *in piú di un nodo* questa funzione. La risposta è solo in parte affermativa: se, per esempio, interpoliamo la funzione nell'intervallo $[-5, +5]$ in n punti equidistanti la successione dei polinomi $P_n(x)$ converge a $1/(1+x^2)$ in $[-3, +3]$, ma diverge per $|x|\geq 4$. Agli inizi del Novecento Poincaré metteva in guardia contro gli eccessi in tale direzione che finivano col generare mostri e additava la piaga delle funzioni continue senza derivata [Poincaré 1908, pp. 131 sgg.]. Ma non c'è bisogno di spingersi cosí oltre; la funzione del fenomeno di Runge fa ancora parte del cantuccio delle funzioni buone: la *foi du charbonnier* è una cattiva compagna di strada già nella piú consueta pratica matematica.

Dobbiamo quindi concludere che, anche sul terreno del calcolo, ci siamo imbattuti in un museo teratologico [*ibid.*, p. 133]? Una situazione è in realtà paradossale proprio nella misura in cui *sembra essere* non vera in base a idee

preconcette [Meschkowski 1960, trad. it. p. 71]. Nel caso il preconcetto è quello che porta – specie nelle applicazioni – «ad accettare come "evidente" ciò che non lo è affatto e a dimenticare che la nostra "intuizione" è uno strumento piuttosto rudimentale, che ci inganna grossolanamente alla prima occasione» [Dieudonné 1968, p. 10].

La contrapposizione intuizione/rigore è però mobile: la scoperta di un paradosso apre la strada a metodi piú produttivi, anche se il cammino non è sempre lineare. Nella fattispecie l'ostacolo è la convinzione non critica che la simulazione «piú accorta» o «piú fedele» dell'andamento complessivo di una funzione si basi necessariamente sulla scelta di nodi equidistanti che per $n \to \infty$ si addensano nell'intervallo di base. Piú adeguata si rivela invece una diversa scelta dei nodi.

Si ha infatti, per un teorema enunciato da Bernstein nel 1916, che, nell'ipotesi che per la funzione f continua in $I=[a, b]$ esiste la derivata f' limitata in I, allora in I convergono uniformemente ad f i polinomi di interpolazione formati nei nodi di Čebyšev:

$$x_k = \frac{b+a}{2} + \frac{b-a}{2} \cos \frac{k\pi}{n+1} \qquad k=0, 1, \ldots, n+1.$$

2. *Polinomi ortogonali.* Una famiglia di polinomi $(\omega_n)_{n\geq 0}$ costituisce una famiglia ortogonale rispetto alla funzione peso $\omega(x)$ nell'intervallo $[a, b]$ se per due polinomi qualunque si ha:

$$\int_a^b \varphi_n(x)\, \varphi_m(x)\, \omega(x)\, dx = 0 \qquad \text{quando } n \neq m$$

$$\int_0^b \varphi_n^2(x)\, \omega(x)\, dx \neq 0.$$

Lo sviluppo di una funzione $f(x)$ in termini di polinomi ortogonali è assai utile poiché i polinomi ortogonali sono in generale facili da manipolare, hanno buone proprietà di convergenza e forniscono una rappresentazione ben condizionata della funzione.

Il principio dell'approssimazione di una funzione in tale ambito è basato su di un'estensione del metodo dei minimi quadrati; in effetti si approssima f con $f^*(x) = c_0\, \varphi_0(x) + c_1\, \varphi_1(x) + \ldots + c_n\, \varphi_n(x)$ ed i coefficienti $c_0, c_1, \ldots, c_n$ sono determinati con la condizione che $\| f^* - f \|^2 = \int_a^b |f^*(x) - f(x)|^2 \omega(x)\, dx$ sia minimo. L'esistenza dei coefficienti $c_0, c_1, \ldots, c_n$ è un fatto caratteristico degli spazi di Hilbert e i coefficienti c_j sono determinati dalle formule

$$c_j = \frac{(f \mid \varphi_j)}{\|\varphi_j\|^2} \qquad j=0, 1, \ldots, n$$

che costituiscono l'analogo delle formule per la determinazione dei coefficienti dello sviluppo in serie di Fourier.

Fra la fine del Settecento e la metà dell'Ottocento sono state costruite alcune famiglie notevoli di polinomi ortogonali quali i polinomi di Čebyšev, quelli di Legendre e quelli di Gram.

4.7. Metodi degli elementi finiti.

I metodi degli elementi finiti sono fra i metodi attualmente piú usati per risolvere i problemi di meccanica delle strutture di cui il problema di Dirichlet considerato nel § 3.8 è il caso particolare forse piú semplice. Tali metodi si sono sviluppati impetuosamente a partire dalla metà degli anni '50 nell'ambito degli ingegneri, ma i risultati sulla maggiorazione degli errori, che costituiscono uno degli aspetti piú nuovi e interessanti della teoria, sono stati ottenuti solo nell'ultimo decennio dopo un primo lavoro di Zlamal (1968), anche se Courant in un lavoro pionieristico (1943) aveva già considerato tale problematica.

Ricordando la seconda e la terza formulazione del problema, l'idea principale dell'approssimazione interna (cfr. anche l'articolo «Approssimazione» di questa stessa *Enciclopedia*, §§ 2.2, 2.4 e 2.5) consiste nel prendere un sottospazio V_N di V di dimensione finita e nel risolvere il problema approssimato

(16) Dato f cercare $u_N \in V_N$ tale che $a(u_N, v) = (f, v)$ per ogni $v \in V_N$.

Tale problema, che ammette una soluzione unica u_N, è equivalente alla soluzione di un sistema lineare di dimensione finita N. Infatti se $\{w_i^N \mid i=1, \ldots, N\}$ è una base di V_N allora $u_N = \sum_{i=1}^N \xi_i w_i^N$ dove i coefficienti si ottengono risolvendo il sistema lineare (che scriveremo per semplicità $A_N u_N = f_N$)

$$(17) \qquad \sum_{i=1}^N a(w_i^N, w_j^N)\, \xi_i = (f, w_j^N) \qquad j=1, \ldots, \dim V_N$$

I problemi che si pongono sono allora i seguenti:

a) determinare una maggiorazione (se possibile ottimale in un senso opportuno, cfr. «Approssimazione», § 2.1, p. 779) dell'errore $\varepsilon(V_N) = \|u - u_N\|_{1,\Omega}$ quando la dimensione di V_N tende all'infinito;

b) costruire concretamente dei sottospazi V_N per i quali tale maggiorazione sia valida;

c) risolvere il sistema (17) dopo averne calcolato i coefficienti ed il termine noto.

Indichiamo brevemente un esempio di costruzione di sottospazi V_N; a tal fine sia Ω un poligono limitato del piano e si costruisca una triangolazione $\mathcal{T}$ di Ω tale che l'intersezione di due triangoli sia vuota, o ridotta ad un vertice, o ridotta ad un lato comune (e in questo caso i due triangoli sono detti adiacenti).

In corrispondenza di ogni triangolo K si consideri un insieme finito $\Sigma = \{a_1, \ldots, a_d\}$ di punti detti nodi ed uno spazio vettoriale P_K di dimensione

finita formato di funzioni definite su K con la condizione che ogni $\varphi \in P_K$ sia determinata per interpolazione di Lagrange dai valori $\varphi(a_i)$, $i=1, \ldots, d$. Gli elementi della base di P_K sono detti funzioni di forma dell'elemento finito $\{K, \Sigma, P_K\}$. Per esempio se K è un triangolo di vertici a_1, a_2, a_3 si può prendere $\Sigma = \{a_1, a_2, a_3\}$ e $P_K = \{\varphi(x, y) \mid \varphi(x, y) = \alpha + \beta x + \gamma y\}$; risulta allora $\dim P_K = 3$; si possono anche considerare i polinomi di secondo grado ed allora Σ è formato da a_1, a_2, a_3 e dai punti medi dei lati.

Si assume allora come sottospazio $V_N = \{v \in V \mid$ per ogni triangolo K la restrizione di v a K è in $P_K\}$.

Nella pratica si assume un triangolo di riferimento $\hat{K}$ con relativo insieme $\hat{\Sigma}$ e spazio $\hat{P}_{\hat{K}}$ ed il passaggio da $\hat{K}$ a K triangolo generico è fatto con una trasformazione affine che deve indurre un isomorfismo di $\hat{P}_{\hat{K}}$ su P_K.

È facile ora costruire una base di V_N; basta infatti per ogni nodo j della reticolazione considerare la funzione w_j che ivi vale 1 e vale 0 in tutti gli altri nodi. Si tratta di funzioni $\neq 0$ sul triangolo K solo se il nodo $j \in K$, e in tale caso w_j coincide con una delle funzioni di forma di P_K. I coefficienti della matrice A_N diventano allora

$$a(w_i, w_j) = \int_\Omega T \left\{ \frac{\partial w_i}{\partial x} \frac{\partial w_j}{\partial x} + \frac{\partial w_i}{\partial y} \frac{\partial w_j}{\partial y} \right\} dx\, dy =$$

$$= \sum_{K \in \mathcal{T}} \int_K T \left\{ \frac{\partial w_i}{\partial x} \frac{\partial w_j}{\partial x} + \frac{\partial w_i}{\partial y} \frac{\partial w_j}{\partial y} \right\} dx\, dy =$$

$$= \sum_{K \in \mathcal{P}_i \cap \mathcal{P}_j} \int_K T \left\{ \frac{\partial w_i}{\partial x} \frac{\partial w_j}{\partial x} + \frac{\partial w_i}{\partial y} \frac{\partial w_j}{\partial y} \right\} dx\, dy$$

dove $\mathcal{P}_i = \{K \mid i$ è un nodo di $K\}$ e quindi $a(w_i, w_j) \neq 0$ solo se $\mathcal{P}_i \cap \mathcal{P}_j \neq \emptyset$ e cioè solo se esiste K con $i, j \in K$. Ciò significa che la matrice è sparsa e questo fatto è di grande importanza per la risoluzione numerica di (17) (nonché per la memorizzazione dei coefficienti).

Per quanto riguarda la maggiorazione dell'errore si consideri una successione di triangolazioni $\mathcal{T}_n$, $n = 1, 2, \ldots$, tale che detto h_n il piú grande diametro dei triangoli di $\mathcal{T}_n$ risulti $\lim_{n \to \infty} h_n = 0$ e tale che, detto $\vartheta(K)$ il piú piccolo angolo al vertice di K, risulti $\vartheta(K) \geq \vartheta^* > 0$ per ogni $K \in \mathcal{T}_n$ e per $n = 1, 2, \ldots$ Sotto ragionevoli ipotesi di regolarità per la soluzione del problema esatto, si dimostra che $\|u - u_n\|_{1,\Omega} = O(h_n)$ nel caso di polinomi lineari e $\|u - u_n\|_{1,\Omega} = O(h_n^2)$ nel caso di polinomi quadratici dove ovviamente u_n è la soluzione approssimata corrispondente alla triangolazione $\mathcal{T}_n$. Se inoltre il rapporto fra il piú grande e il piú piccolo diametro dei triangoli di $\mathcal{T}_n$ è limitato uniformemente rispetto a n, è possibile provare che tali maggiorazioni sono asintoticamente ottimali.

Ma tali risultati hanno interesse prevalentemente teorico perché nella pratica ci si arresta dopo aver fatto poche triangolazioni successive. Inoltre una loro limitazione è costituita dal fatto che in essi si suppone di aver calcolato esattamente i coefficienti $a(w_i, w_j)$ eseguendo in modo esatto l'integrazione; qualora ciò non avvenga, ma si usino opportune formule di integrazione numerica, le maggiorazioni dell'errore precedenti sono ancora valide, anche se non è provata la loro asintotica ottimalità.

Per quanto riguarda la soluzione del sistema (17) si possono applicare le considerazioni del § 4.4 tenendo naturalmente conto delle proprietà speciali della matrice A_N; siccome per esempio tale matrice è sparsa, si dimostra che il numero delle operazioni per risolvere il sistema è $O((\dim V_N)^2)$ e non $O((\dim V_N)^3)$. Per quanto riguarda il condizionamento della matrice A_N esso dipende fortemente da Ω, dalla triangolazione e dall'ordinamento dei nodi; in ogni caso esso cresce e quindi peggiora al diminuire di h_n.

Per ulteriori sviluppi, si vedano Strang e Fix 1973, e Ciarlet 1978.

4.8. Metodi numerici per problemi di evoluzione: consistenza, stabilità, convergenza.

Riesaminiamo ora sotto il profilo del calcolo numerico alcuni argomenti delineati nei §§ 3.7 e 3.8.

1. *Equazioni differenziali ordinarie.* Riprendiamo il problema di Cauchy (o dei valori iniziali), studiato nel § 3.7; determinare una soluzione di

$$(18) \qquad \begin{cases} \dfrac{dy}{dt} = f(t, y) \\ y(a) = c \end{cases}$$

con f tale che $|f'_y| \leq L$.

La soluzione di tale problema può essere considerata come una funzione $y(t, c)$ dove c è la condizione iniziale; al variare di c si avrà una famiglia di curve nel piano y, t. Pur essendo il problema ben posto, la dipendenza di $y(t, c)$ da c è tuttavia di grande importanza nel trattamento numerico dell'equazione differenziale; e per esempio, nei cosiddetti metodi numerici ad un passo, quale appunto il metodo di Eulero visto nel § 3.7, si procede passo dopo passo nel calcolo di valori approssimati $y_1, y_2, \ldots$ di $y(t_1), y(t_2), \ldots$ introducendo a ogni passo una piccola perturbazione – dovuta agli errori di troncatura e/o di arrotondamento – che produce il passaggio di $y(t)$ ad un'altra «pista» nella famiglia delle curve integrali.

Si può confrontare il processo precedente ad un processo di interesse; ad ogni tappa si paga un «interesse» sugli errori commessi in precedenza. Al tempo stesso un nuovo «capitale di errore» (errore locale) è aggiunto. È possibile tuttavia che la «rata di interesse» sia negativa, il che costituisce un guadagno in questo ambito.

Se le curve nella famiglia delle soluzioni si allontanano l'una dall'altra rapidamente, il problema di Cauchy è mal condizionato, altrimenti esso è ben condizionato [Dahlqvist, Björck e Anderson 1974, pp. 334-35].

In questo contesto è fondamentale distinguere fra *errore* di discretizzazione locale ed errore globale. L'errore globale nel punto t_{n+1} è $y_{n+1}-y(t_{n+1})$ dove $y(t_{n+1})$ è la soluzione esatta del problema di Cauchy (18). L'errore locale in t_{n+1} è la differenza fra il valore calcolato y_{n+1} ed il valore in t_{n+1} della curva integrale che passa per $\langle y_n, t_n\rangle$.

Piú in generale si parla di metodi a passo multiplo (a k passi) quando il valore y_n è approssimato usando i valori $y_{n-1}, y_{n-2}, \ldots, y_{n-k}$, risolvendo l'equazione

$$(19) \qquad \sum_{i=0}^{k} (\alpha_i y_{n-i} - h\beta_i f(t_{n-i}, y_{n-i})) = 0 \qquad \text{con } \alpha_k\alpha_0 \neq 0.$$

Naturalmente per utilizzare un tale metodo bisogna conoscere i valori di partenza $y_0, \ldots, y_{k-1}$. Se $\beta_0 \neq 0$ allora il metodo è implicito e ad ogni tappa bisogna risolvere una equazione non-lineare usando i metodi dal § 4.5.

Introduciamo ora le seguenti definizioni fondamentali: fissato $h>0$, denotiamo con $\mathcal{J}_h$ l'insieme degli interi $n \geq 0$ tali che $t_n = t_0 + nh \leq T$. Ciò premesso: il metodo (19) è detto consistente se l'errore locale di discretizzazione è infinitesimo e cioè se per ogni funzione f con $|f'_y| \leq L$ e per ogni curva integrale di (18)

$$\lim_{h\to 0} \frac{1}{h} \max_{n\in\mathcal{J}_h} \left| \sum_{i=0}^{k} (\alpha_i y(t_{n-i}) - h\beta_i f(t_{n-i}, y(t_{n-i})))\right| = 0$$

(cfr. anche «Approssimazione», § 2.4, pp. 781-82).

Il metodo (19) è detto convergente se l'errore globale è infinitesimo, e cioè se per ogni f con $|f'_y| \leq L$ risulta $\max_{n\in\mathcal{J}_h} |y_n - y(t_n)|$ infinitesimo per h tendente a zero, comunque siano scelti i valori di partenza purché $\lim_{n\to 0} y_i = c$, per $i = 0, \ldots, k-1$.

Il metodo è detto stabile se per ogni funzione f con $|f'_y| \leq L$ e comunque siano scelti i valori di partenza purché $|y_i| \leq M$ per $i = 0, \ldots, k-1$ la famiglia delle soluzioni y_n è uniformemente limitata per n tendente a zero e cioè esiste M_1 dipendente da M tale che per ogni $h>0$ e $h<h_0$ si ha $\max_{n\in\mathcal{J}_h} |y_n| \leq M_1$ (cfr. anche «Approssimazione», § 2.5, p. 785).

I risultati chiave in questo contesto sono allora i seguenti teoremi:

a) Il metodo (19) è convergente se e solo se esso è stabile e consistente.
b) Una condizione necessaria e sufficiente per la stabilità è che ogni radice in $\mathbf{c}$ del polinomio $\rho(z) = \alpha_0 z^k + \ldots + \alpha_k$ verifichi $|z_i| \leq 1$ e le radici verificanti $|z_i| = 1$ abbiano molteplicità uno.
c) Una condizione necessaria e sufficiente per la consistenza è che $\rho(1) = 0$ ed inoltre $\rho'(1) = \sigma(1)$ ove $\sigma(z) = \beta_0 z^k + \ldots + \beta_k$.

La dicotomia continuo/discreto che abbiamo visto emergere ogniqualvolta si segue l'approccio numerico ai problemi classici porta dunque nel contesto esaminato in questa sezione (problemi di evoluzione) alla coppia locale/globale. Prendiamo per esempio il teorema *a*): esso autorizza appunto a passare da

un controllo dell'errore locale al controllo dell'errore globale mediante una condizione supplementare (la stabilità, anch'essa indipendente dalla conoscenza della soluzione del problema). Proprio un'argomentazione del genere motiva un criterio generale – noto come principio di Lax – secondo cui nei problemi di evoluzione (ordinari e alle derivate parziali, lineari e non-lineari, ecc.) consistenza e stabilità implicano la convergenza.

Relativamente al condizionamento del problema (18), e soprattutto del suo analogo nel caso in cui y sia un vettore, osserviamo che esso dipende dalla costante L. Il problema di Cauchy è mal condizionato se tale costante L è grande e se inoltre

$$-f'_y(t, y) \geq a \geq 0 \qquad \text{per ogni } y \text{ e per ogni } t \in [0, T];$$

in tale caso si parla anche di equazione differenziale *stiff*. Illustriamo su di un esempio il tipo di difficoltà che si incontrano in tale situazione. Data g continua con la derivata prima in $[0, T]$ si consideri il problema di Cauchy per l'equazione differenziale lineare

$$\begin{cases} y' = -\lambda(y - g(t)) + g'(t) \\ y(0) = y_0 \end{cases}$$

ove λ è un numero reale ≥ 0, la cui soluzione è

$$y(t) = (y_0 - g(0))e^{-\lambda t} + g(t).$$

Supponiamo λ molto grande, $y_0 \neq g(0)$ e $g(t)$ funzione che varia lentamente e sempre $\geq c_1 > 0$; allora la soluzione $y(t)$ presenta un regime transitorio iniziale in cui $y''(t)$ è dell'ordine di λ^2; peraltro dopo un tempo dell'ordine di $1/\lambda$ il contributo del termine $e^{-\lambda t}$ diviene trascurabile e la soluzione si comporta essenzialmente come la funzione $g(t)$: si tratta del cosiddetto regime stazionario. Se viene utilizzato il metodo esplicito di Eulero (cfr. § 3.7) per il quale $\rho(z) = z - 1$ e $\sigma(z) = 1$ il corrispondente errore locale di discretizzazione risulta

$$\begin{aligned} \varepsilon_{n-1} &= y(t_n) - y(t_{n-1}) - (t_n - t_{n-1}) f(t_{n-1}, y_{n-1}) = \\ &= y(t_n) - y(t_{n-1}) - (t_n - t_{n-1}) y'(t_{n-1}) = \\ &= \frac{(t_n - t_{n-1})^2}{2} y''(\vartheta_n) \end{aligned}$$

con $t_{n-1} < \vartheta_n < t_n$. Tenendo allora conto della forma dell'equazione di questo esempio si ottiene per induzione la seguente espressione per l'errore globale:

$$e_n = y(t_n) - y_n = \sum_{l=0}^{n-1} \varepsilon_l \prod_{k=l+1}^{n-1} (1 - \lambda \Delta t_k)$$

ove si è posto $\Delta t_k = t_{k+1} - t_k$. Appare quindi naturale scegliere un passo Δt_n variabile e cioè molto piccolo finché $\lambda^2 \Delta t_n$ è molto minore di 1 ed un passo molto piú grande nel regime stazionario. Purtroppo tuttavia se ε_n è piccolo $|1 - \lambda \Delta t_n|$ diviene molto grande e quindi gli errori commessi per $t_l < t_n$ sono amplificati in maniera catastrofica. Ciò significa che il metodo di Eulero esplicito è inadeguato

alla risoluzione delle equazioni differenziali mal condizionate. Come ha provato Dahlqvist nel 1963, è questa la situazione di tutti i metodi lineari a passo multiplo espliciti ed anche di quelli impliciti piú accurati. Piú adeguati in questo contesto si sono rivelati invece i metodi impliciti del tipo di Runge-Kutta.

2. *Equazione del calore.* Riprendiamo il problema considerato nel § 3.8 della diffusione del calore:

$$\begin{cases} \dfrac{\partial \vartheta}{\partial t} = a \dfrac{\partial^2 \vartheta}{\partial x^2} & 0<x<l \quad 0<t<T \\ \vartheta(x, 0) = \vartheta_0(x) & 0<x<l \\ \vartheta(0, t) = \vartheta(l, t) = 0 & t>0 \end{cases}$$

e introduciamo una discretizzazione nel tempo con passo $\Delta t>0$ e nello spazio con passo $\Delta x = l/I$; l'approssimazione di $\vartheta(i\,\Delta x, n\,\Delta t)$ verrà indicata con $\vartheta_{i,n}$. L'equazione a derivate parziali viene sostituita dall'equazione alle differenze finite per $i=1, \ldots, I$ ed $n \geq 0$

$$\frac{\vartheta_{i,n+1} - \vartheta_{i,n}}{\Delta t} = a \frac{\vartheta_{i+1,n} - 2\vartheta_{i,n} + \vartheta_{i-1,n}}{(\Delta x)^2} \qquad \text{(metodo esplicito)}$$

oppure

$$\frac{\vartheta_{i,n+1} - \vartheta_{i,n}}{\Delta t} = a \frac{\vartheta_{i+1,n+1} - 2\vartheta_{i,n+1} + \vartheta_{i-1,n+1}}{(\Delta x)^2} \qquad \text{(metodo implicito).}$$

Tali equazioni sono rappresentate schematicamente sul reticolo di discretizzazione (cfr. fig. 25).

A tali equazioni vanno aggiunte le condizioni iniziali

$$\begin{aligned} \vartheta_{i0} &= \vartheta_0(i\,\Delta x) & i &= 0, \ldots, I \\ \vartheta_{0n} &= 0_{In} = 0 & n &= 0, 1, 2, \ldots \end{aligned}$$

Introdotto il vettore $\vartheta_n = \langle \vartheta_{1,n}, \vartheta_{2,n}, \ldots, \vartheta_{I-1,n} \rangle$ e posto $\lambda = a\,\Delta t/(\Delta x)^2$ i metodi esplicito e implicito possono scriversi come sistemi lineari

$$\begin{aligned} \vartheta_{n+1} &= A\vartheta_n & &\text{metodo esplicito} \\ B\vartheta_{n-1} &= \vartheta_n & &\text{metodo implicito.} \end{aligned}$$

Nel caso del metodo esplicito la matrice tridiagonale A di ordine $(I-1)$ è ottenuta mediante la formula

$$A = \begin{pmatrix} 1-2\lambda & \lambda & 0 & \ldots & 0 & 0 \\ \lambda & 1-2\lambda & \lambda & \ldots & 0 & 0 \\ 0 & \lambda & 1-2\lambda & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1-2\lambda & \lambda \\ 0 & 0 & 0 & \ldots & \lambda & 1-2\lambda \end{pmatrix}$$

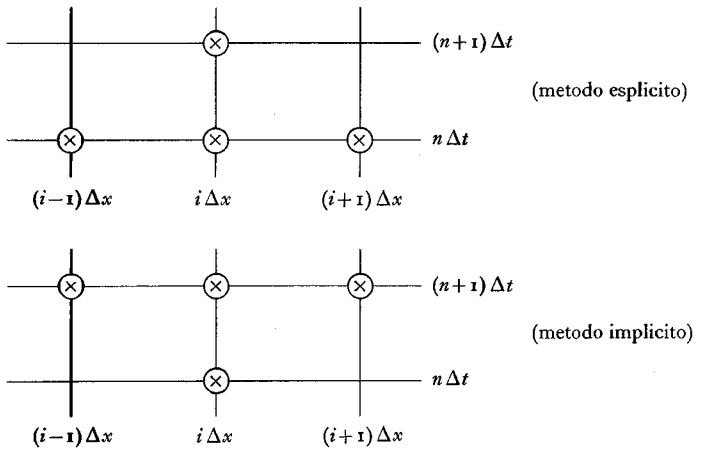


Figura 25.
Reticolo di discretizzazione.

mentre nel caso del metodo implicito la matrice invertibile B di ordine $(I-1)$ è

$$B = \begin{pmatrix} 1+2\lambda & -\lambda & 0 & \ldots & 0 & 0 \\ -\lambda & 1+2\lambda & -\lambda & \ldots & 0 & 0 \\ 0 & -\lambda & 1+2\lambda & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1+2\lambda & -\lambda \\ 0 & 0 & 0 & \ldots & -\lambda & 1+2\lambda \end{pmatrix}$$

Le approssimazioni assunte sono consistenti nel senso che per $\Delta t \to 0$ e $\Delta x \to 0$ l'errore locale di discretizzazione tende a zero.

Si dirà poi che l'approssimazione è stabile se esiste una costante $M>0$ tale che per ogni $n \geq 1$, per ogni vettore ϑ_0 e per ogni Δt e Δx risulta

$$\|\vartheta_n\| \leq M \|\vartheta_0\| \tag{20}$$

per una opportuna norma dei vettori (per esempio la norma euclidea); l'approssimazione è convergente se per ogni $x_0 \in (0, l)$ e $t_0>0$ $|\vartheta(i\,\Delta x, n\,\Delta t) - \vartheta_{in}|$ tende a 0 quando Δt tende a 0 e Δx tende a 0 in modo che $i\,\Delta x$ tende a x_0 e $n\,\Delta t$ tende a t_0.

Il teorema fondamentale di Lax-Richtmyer (1956) asserisce allora che se lo schema alle differenze finite è stabile e consistente allora l'approssimazione trovata è convergente.

I due metodi considerati sono entrambi consistenti; per quanto riguarda la stabilità osserviamo che risulta $\vartheta_n = A^n \vartheta_0$ (metodo esplicito) e $\vartheta_n = B^{-n} \vartheta_0$

(metodo implicito) e quindi la maggiorazione a priori (20) risulta verificata se e solo se gli autovalori di A sono in modulo ≤ 1 (rispettivamente quelli di B sono in modulo ≥ 1). È facile mostrare che mentre B è incondizionatamente stabile comunque si scelgano Δt e Δx il metodo esplicito è stabile se e solo se $a\,\Delta t/(\Delta x)^2 \leq 1/2$, condizione ottenuta per la prima volta da Courant-Friedrichs-Lewy nel 1928 in un lavoro pioneristico sulla convergenza delle soluzioni delle equazioni alle differenze finite quando $\Delta t \to 0$ e $\Delta x \to 0$.

3. *Equazioni delle onde.* Le considerazioni svolte per l'equazione del calore si adattano anche all'equazione delle onde; ricordiamo che anche in tal caso vale il teorema di Lax-Richtmyer. Senza entrare nei dettagli osserviamo solo che la condizione di stabilità nel metodo esplicito s'interpreta in termine di triangolo d'influenza: il triangolo numerico di influenza dev'essere piú grande di quello continuo (e cioè $c\,\Delta t/\Delta x \leq 1$: è la condizione di Courant-Friedrichs-Lewy).

Possiamo concludere questo paragrafo riprendendo il paradigma di Joseph Fourier; per questi giudice ultimo della bontà di un modello era l'accordo con l'esperienza. In una prospettiva che contempla un approccio pluralistico allo studio di un processo, accuratezza e attendibilità vanno intese in un'accezione piú sfumata. «È chiaramente inadeguato valutare i risultati esclusivamente sulla base degli errori introdotti dal metodo numerico. Spesso questi errori sono molto piú piccoli di quelli dovuti a precedenti decisioni circa le formulazioni matematiche usate nel modellizzare il problema assegnato. L'accuratezza dei risultati numerici dovrebbe dunque essere una misura della loro deviazione dalla soluzione di un modello matematico "superiore". Inoltre questi risultati possono venir considerati attendibili solo se i cambiamenti nel modello di riferimento e, piú in generale, nell'intera sequenza di passi dalla formulazione del problema all'esito finale hanno effetti relativamente piccoli. Questo concetto di attendibilità è di importanza centrale. Al confronto l'accuratezza dei risultati svolge un ruolo secondario» [Babuška e Rheinboldt 1977, pp. 3-4]. La concezione sofisticata dell'attendibilità dei risultati lascia dunque al ricercatore una maggiore autonomia della concezione di Fourier: uno studio attento degli schemi matematici impiegati e controlli ben pianificati [nel senso chiarito dalla citazione di Babuška e Rheinboldt 1977] permettono significativi approfondimenti delle questioni in esame senza troppa preoccupazione per gli stessi errori introdotti usando un particolare metodo numerico. Ma è altrettanto naturale che un approccio del genere metta in primo piano il problema del costo delle computazioni e quindi della mediazione con le esigenze di attendibilità e accuratezza, ecc. Si tratta, ancora una volta, di definire ciò che è «ottimale»: il che ci rimanda di nuovo alla dinamica concreto/astratto (in modo analogo a come indicato nel § 2.6).

5. *L'esplicazione del concetto di calcolabilità.*

5.1. Posizione del problema.

Nel § 4 abbiamo incontrato una vasta gamma di problemi che venivano risolti trovando in modo effettivo dei risultati numerici. A ogni problema veniva associato (almeno) un opportuno algoritmo. Chiediamoci ora se è possibile dare una caratterizzazione generale di applicazione di $\mathbf{N}^k$ in $\mathbf{N}$ calcolabile in modo effettivo o, come altri dice, computabile. Abbiamo visto molte applicazioni di $\mathbf{N}^k$ in $\mathbf{N}$ (o sostanzialmente riconducibili ad applicazioni del genere) di fatto calcolate. Ma in questa sede non poniamo la questione «di fatto», ma quella «di diritto», quella cioè di una definizione sufficientemente rigorosa della computabilità di un'applicazione intesa come proprietà *intrinseca*, non dipendente quindi dalle capacità umane e tecnologiche dispiegate nella pratica del calcolo.

L'esempio che segue mostra che ci stiamo collocando a un livello di astrazione maggiore che nel § 4. Definiamo infatti con esattezza un'applicazione senza che ciò comporti asserzioni circa il modo e/o la possibilità di calcolarla: ciò rientra perfettamente nello spirito di tutta quella pratica che si basa sulla nozione di applicazione comunemente accettata in matematica (per esempio nel contesto della teoria degli insiemi: cfr. anche l'articolo «Applicazioni» di questa stessa *Enciclopedia*, § 2). Sia allora $F(n) = 1$ se esistono numeri naturali diversi da 0, x, y, z tali che $x^n + y^n = z^n$, $F(n) = 0$ altrimenti. Anche se sono noti molti valori della F (per esempio $F(0) = 0$, $F(1) = 1$, $F(2) = 1$, $F(3) = F(4) = \ldots = F(4002) = 0$) non sappiamo ancora se per F esista per cosí dire una ricetta per ricavare valori in $\mathbf{N}$ da argomenti in $\mathbf{N}$, cioè una procedura effettiva di calcolo. (L'applicazione F corrisponde infatti al celebre problema posto dall'«ultima congettura» di Fermat: «Non è possibile dividere un cubo in due cubi, o un biquadrato in due biquadrati, né, in generale, alcun'altra potenza di grado superiore al secondo in due altre potenze dello stesso grado; della qual cosa ho scoperto una dimostrazione veramente mirabile che non può essere contenuta nella ristrettezza del margine» [1670, trad. it. p. 18]).

Ma cosa intendiamo per «procedura effettiva»? Se un «computista», una volta messo alla prova nel calcolo di una applicazione numerica, è anche in grado di fornire ogni volta il valore giusto della funzione aritmetica, questo fatto non depone ancora a favore della computabilità di detta funzione: egli deve ancora dirci in che modo procede e altre persone debbono poter apprendere il procedimento (il computista potrebbe fruire di una sorta di «intuizione bergsoniana»!): l'usuale *desideratum* di intersoggettività nella pratica scientifica prende qui la forma della richiesta dell'esibizione di un *testo* in cui vengono scritti tutti i passaggi del calcolo in modo comprensibile e controllabile.

5.2. Macchine di Turing e tesi di Church.

Per chiarire quest'ultimo punto supponiamo che un calcolatore (uomo o macchina non ha importanza, dato che il nostro è, dopo tutto, una sorta di

«esperimento mentale») scriva i suoi numeri in una forma standard (già questa richiesta è essenziale: se nell'esempio del § 5.1 fosse assegnato il calcolo $F(7^{7^7})$, il calcolatore potrebbe «non capire» questo tipo di rappresentazione e non farebbe quindi alcun conto): i numeri vengono rappresentati, per esempio, da sequenze di segni 1, piú precisamente $n+1$ tacche per rappresentare il naturale n (anche lo 0 infatti è elemento di **N**) e supponiamo ancora di disporre di un nastro potenzialmente infinito, diviso in quadrati tutti uguali o celle in modo da poter collocare un solo segno 1 per cella, pressappoco come faceva il troglodita quando incideva sulla parete della caverna una tacca per ogni oggetto che voleva contare. A questa notazione a tacche per i numeri (piú semplice delle stesse scritture binarie per le macchine calcolatrici o decimali per gli esseri umani) aggiungeremo un segno, per esempio $*$ (detto *blank*), che verrà utilizzato per distinguere una sequenza di 1 rappresentante un numero qualsiasi da un'altra rappresentazione di un secondo numero.

Ciò premesso, concepiremo il nostro calcolatore come un dispositivo che esamina il nastro che scorre, poniamo da sinistra a destra. Il dispositivo esegue queste quattro operazioni-base: 1) può scrivere 1 nella cella che sta esaminando se 1 non compare già in tale cella; 2) può cancellare 1 nella cella che sta esaminando, mettendoci il *blank* se già non c'è; 3) può spostare la sua attenzione a una cella a sinistra (tecnicamente: spostando di una cella il nastro verso destra); 4) può spostare la sua attenzione a una cella a destra (tecnicamente: spostando di una cella il nastro verso sinistra). Eseguire un'operazione-base costituisce un passo del calcolo e alla conclusione di ogni passo il nostro dispositivo assume un solo stato tra un insieme finito di stati possibili. Se denotiamo con q_i, $i=0, 1, 2, \ldots$, tali stati distinti e indichiamo con I, B, D, S le operazioni-base 1), 2), 3), 4) rispettivamente, possiamo formulare l'insieme delle regole che determinano il comportamento del dispositivo come un insieme di quadruple, consistenti ciascuna di simboli di I) uno stato, II) una possibile condizione della cella (0 1 0 $*$), III) un'operazione-base, IV) uno stato, in modo che una quadrupla (I, II, III, IV) esprima la regola che dati I) e II) il dispositivo esegue III) e si sposta su IV), con l'unica restrizione (coerenza) che due quadruple distinte devono differire per I) e per II), in modo da evitare che l'insieme delle regole autorizzi due differenti modi di procedere al medesimo istante. Ammettiamo infine che il dispositivo possa in certe circostanze non eseguire alcuna operazione (stop).

Questa caratterizzazione comportamentistica del calcolo venne data da Turing (1936). Una macchina di Turing non è null'altro che l'insieme delle quadruple che descrivono il comportamento di un dispositivo come quello sopra descritto: piú precisamente un qualsiasi insieme di quadruple che usi un qualsiasi numero (finito) di stati costituisce una macchina di Turing, purché soddisfi la restrizione della coerenza. Data una macchina di Turing, un nastro, una cella sul nastro e uno stato iniziale, la macchina di Turing esegue una sequenza di operazioni univocamente determinate, che può terminare o può non aver termine in un numero *finito* di passi. Per rappresentare un naturale n come «entrata» si segnano in sequenza $n+1$ tacche sul nastro; si fa partire la macchina

dallo stato q_0 della cella piú a sinistra che contiene un 1: il numero naturale di «uscita» sarà il numero totale degli 1 che appaiono ovunque nel nastro prima del $*$ seguente quando (e *se*) la macchina si ferma.

Piú astrattamente, una macchina di Turing può venir identificata con un'applicazione di un sottoinsieme finito di $\mathbf{N} \times T$ in $U \times \mathbf{N}$ ove l'insieme dei naturali **N** fornisce degli indici per gli stati, $T=\{0, *\}$ rappresenta le condizioni possibili di una cella del nastro e $U=\{I, B, D, S\}$.

Che il procedimento con una macchina siffatta sembri già troppo prolisso per calcoli notevolmente semplici in linea di principio non ha molta importanza. Si può avere semmai qualche perplessità di fronte al fatto che per ogni applicazione di **N** in **N** calcolabile in modo effettivo occorre una particolare macchina di Turing: detto in breve, ogni macchina di Turing calcola solo una funzione, mentre le calcolatrici automatiche reali sono universali e possono venir adattate a una vasta gamma di problemi mediante un'opportuna programmazione. Ma poiché una macchina di Turing viene identificata con una tabella di istruzioni (tale è infatti l'interpretazione naturale delle applicazioni di sottoinsiemi finiti di $\mathbf{N} \times T$ in $U \times \mathbf{N}$), una tecnica di codificazione permette di assegnare a ogni tabella un numero di catalogo (numero di Gödel della macchina) e pertanto una macchina di Turing, dotata di nastro potenzialmente infinito che contenga i numeri di catalogo di tutte le tabelle e munita di una chiave per l'interpretazione del codice del catalogo, è allora in grado di riprodurre il calcolo per cui è stata progettata la corrispondente macchina di Turing. In altri termini esiste un modo di catalogare tutte le possibili macchine di Turing tale che si può concepire una macchina di Turing universale costruita in modo che quando legge il numero di catalogo di una macchina di Turing particolare può eseguire il calcolo proprio di quella macchina. In questo senso qualsiasi macchina calcolatrice potrebbe essere una macchina di Turing universale *se* sapesse come richiedere un maggior numero di schede perforate e domandare la restituzione di quelle che ha già perforato. Evidentemente quest'ultima condizione è l'equivalente del nastro potenzialmente infinito di una macchina di Turing universale. Nel linguaggio della teoria degli automi (cfr. § 2.8) la coppia formata dalla macchina di Turing e dal suo nastro rappresenta una particolare idealizzazione degli automi finiti e fornisce il paradigma dei cosiddetti automi crescenti.

Dalla opposizione universale/particolare a quella *explicandum*/*explicatum*: come in molte altre discipline scientifiche, anche nella teoria della computabilità vogliamo sostituire a un concetto impreciso, intuitivo, «prescientifico» (*explicandum*: applicazione computabile) un concetto preciso, puntuale, «scientifico» (*explicatum*: applicazioni Turing-computabili, cioè computabili con *una* macchina di Turing particolare o con *la* macchina di Turing universale).

Quello fornito da Turing non è l'unico *explicatum*. A partire dagli anni '30 altri ne sono stati proposti: applicazioni ricorsive generali (Gödel, Kleene), λ-computabili (Church), definibili in termini di sistemi economici (Post), calcolabili con algoritmi di Markov (Andrej A. Markov): ne è nata cosí una teoria rigorosa dell'effettivo. Se qui si è dato un certo spazio alla Turing-computabilità è perché l'approccio di Turing si può motivare in modo estremamente

naturale come un'analisi ideale degli elementi in cui possiamo scomporre l'attività reale del calcolo da parte di un «computista» uomo o macchina che sia. È dunque in tale ottica doppiamente esemplare: vuoi per la chiarezza con cui ricostruisce tale pratica, vuoi per la stessa macchinosità che esso comporta, macchinosità che corrisponde a quella routine che innegabilmente accompagna certe fasi dell'attività di computazione. Ma i teoremi ottenuti negli anni '30 e '40 (Kleene, Church, Turing, Rosser, ecc.) i quali mostrano che gli *explicata* su ricordati, caratterizzanti tutta la stessa classe di applicazioni, sembrano deporre a favore della tesi, formulata da Church nel 1936, che *explicata* del genere sono adeguati, che, cioè, tutte le applicazioni «computabili» sono Turing-computabili (o ricorsive, o calcolabili con algoritmi di Markov, ecc.). Naturalmente si tratta di un argomento di carattere euristico e informale, in quanto la tesi di Church non è, in via di principio, suscettibile di dimostrazione rigorosa proprio perché afferma che hanno la stessa estensione un concetto rigoroso e uno vago. Si possono solo portare argomenti a favore o contro la sua plausibilità. Non è questa la sede per esaminare gli sviluppi connessi alla questione. Ci limitiamo a sottolineare il fatto che attualmente la classe delle funzioni Turing-computabili «è accettata come classe di tutte e solo quelle funzioni per cui si dà una procedura meccanica per ottenere i valori dagli argomenti» [Ritchie 1963, p. 139]. Orbene, «proprio perché tale classe comprende qualsiasi funzione calcolabile, in essa rientrano calcoli arbitrariamente complicati» [*ibid.*] mentre questo non è ovviamente il caso della classe F delle funzioni calcolabili con automi finiti. F costituirà sostanzialmente [per precisazioni di carattere tecnico, cfr. Ritchie 1963, pp. 161-67] «la classe delle funzioni calcolabili nel modo piú immediato possibile». Costruiremo allora una gerarchia di classi di funzioni, tutte ovviamente Turing-computabili ponendo $F_0 = F$ e F_i per $i > 0$ come la classe delle funzioni computabili dalla macchina di Turing che impiegano nei calcoli una quantità di nastro (cioè un numero di celle) limitata da una funzione appartenente a F_{i-1}. È possibile mostrare che per ogni $i = 1, 2, 3, \ldots$ la classe F_i contiene la funzione $f_i(x)$ ove $f_1(x)$ è 2^x e $f_{i+1}(x)$ è definito come $f_1(f_i(x))$ mentre $f_{i+1} \notin F_i$. La gerarchia F_i costituisce una stratificazione di funzioni computabili, che ha un profondo significato intuitivo: ciascuna funzione della classe F_i risulta una funzione la cui complessità computazionale viene «predetta» [Ritchie 1963, p. 139] da una funzione della classe precedente. Si mostra inoltre che $\mathcal{F} = \bigcup_{i=1}^{\infty} F_i$ non coincide con la classe delle funzioni Turing-computabili: è un tipico caso di «sottoricorsività» che gode di alcune proprietà particolarmente interessanti. Ma qui non discutiamo se tali proprietà autorizzino a considerare le funzioni della famiglia $\mathcal{F}$ un correlato formale piú adeguato delle funzioni Turing-computabili [per tale questione e la relativa bibliografia rimandiamo in particolare a Ritchie 1963]. C'interessa invece sottolineare l'analogia con un altro caso particolare di sottoricorsività, quello rappresentato dalla classe delle funzioni dette usualmente ricorsive primitive e introdotte da Kurt Gödel nella celebre memoria del 1931 in cui viene dimostrato il teorema di incompletezza sintattica per l'aritmetica: orbene, tali funzioni

non vengono in tale contesto identificate con le funzioni computabili, ma costituiscono invece quella porzione (molto ristretta) di aritmetica necessaria alla formalizzazione della sintassi di una teoria. Nel caso delle funzioni che appartengono alla famiglia $\mathcal{F}$ (incluse propriamente in quella delle ricorsive primitive [cfr. Ritchie 1963, p. 145]) l'interesse risiede nel fatto che esse permettono di valutare la complessità di un calcolo prevedendone, per cosí dire, la lunghezza.

5.3. Cenni su decidibilità e indecidibilità.

Dopo il breve accenno a certe questioni di sottoricorsività richiamiamo per sommi capi qualche aspetto della teoria della decidibilità. Abbiamo finora considerato applicazioni di **N** in **N**; questa restrizione può però venir abbandonata nel contesto della teoria della ricorsività o (il che è lo stesso, della Turing-computabilità). Nella nozione di algoritmo abbiamo ammesso domini di definizione anche non-numerici e non abbiamo rigidamente specificato che tipo di oggetti tali algoritmi manipolano. In tale caratterizzazione generale la definizione di un algoritmo richiede una preliminare determinazione linguistica dei nomi che vengono assegnati biunivocamente agli oggetti in questione; piú precisamente, un algoritmo dovrà sempre venir definito relativamente a un linguaggio finitamente specificato (ossia con alfabeto finito e con regole finite per la costruzione delle espressioni). Una tecnica usualmente nota come aritmetizzazione (di Gödel) o gödelizzazione permette di normalizzare ogni linguaggio di questo tipo assegnando biunivocamente e in modo effettivo a ogni espressione del linguaggio un numero naturale (il suo numero di Gödel), con il che si giustifica il fatto che ci si limita usualmente (come abbiamo fatto nei §§ 5.1 e 5.2) ad applicazioni di **N** in **N**. La gödelizzazione rappresenta un particolare tipo di codificazione, che permette di estendere al caso generale la teoria delle funzioni Turing-computabili (o delle funzioni ricorsive, ecc.). Ogni algoritmo, infatti, potrà venir considerato allora come descrivente una funzione su numeri; ma, proprio per quanto detto sopra, dovremo servirci, per la definizione dell'algoritmo stesso, di un linguaggio che possegga nomi per i numeri (come abbiamo fatto appunto nei §§ 5.1 e 5.2).

Questo tipo di codificazione è tutt'altro che banale: per esempio i numeri interi e gli stessi numeri razionali ammettono una codificazione del genere (come nel § 3.1, il lettore li pensi come coppie ordinate di naturali, rispettivamente di interi). Invece, alla luce di quanto abbiamo visto nel § 3.3, non esiste un sistema di notazione per i numeri reali. Non possono infatti fungere da nomi per i numeri reali gli sviluppi in base n, per esempio gli usuali sviluppi in base 2, 10, 12, 16, ecc. Lo sviluppo n-ario di x reale è in generale infinito, mentre, come abbiamo specificato piú sopra, un nome è composto invece sempre e soltanto da un numero finito di segni.

Ciò premesso, correliamo alla nozione intuitiva di funzione computabile quella, altrettanto intuitiva, di insieme decidibile: diremo che un qualsiasi insieme $M \subseteq \mathbf{N}$ è decidibile se la sua funzione caratteristica f_M ($f_M(x) = 0$ se $x \notin M$;

$f_M(x)=1$ se $x \in M$) è computabile. Ciò equivale a considerare decidibile M se esiste una procedura effettiva che permette di stabilire per ogni oggetto x se x appartiene a M oppure no. È quindi immediato, accettando la nozione di funzione Turing-computabile come *explicatum* della nozione di funzione computabile, fornire un correlato rigoroso anche per la nozione di insieme decidibile. Non crea problemi estendere la nozione di decidibilità qui introdotta da sottoinsiemi di **N** a sottoinsiemi di $\mathbf{N}^k$.

Come abbiamo già accennato nel § 5.2 è possibile assegnare un numero di Gödel a ogni macchina di Turing. Definiamo allora un insieme $T \subseteq \mathbf{N}$ e una funzione t a valori in **N** nel modo seguente:

- $x \in T$ se e solo se x è il numero di Gödel di una macchina di Turing che calcola una funzione (x è allora detto numero di Gödel della funzione);
- $t(x)=y+1$ se $x \in T$ e y è il valore che assume nel posto x la funzione che ha x come suo numero di Gödel; $t(x)=0$ altrimenti.

Supponiamo che t sia Turing-computabile; allora può venir calcolata da una macchina che ha un certo numero di Gödel, poniamo x_0. Sia $y_0=t(x_0)$: si ha allora $x_0 \in T$ e, stando alla definizione, $t(x_0)=y_0+1$. L'ipotesi che t sia calcolata da una macchina di Turing conduce dunque a una contraddizione. Non è dunque decidibile se una macchina di Turing calcola o no una funzione. Dalla tesi di Church otteniamo subito che la t non è computabile. Naturalmente, poiché l'insieme delle applicazioni di **N** in **N** ha numero cardinale superiore al numerabile, potevamo immediatamente concludere che esistono funzioni non-calcolabili effettivamente. In questo modo non avremmo però dato esplicitamente una funzione di questo tipo, funzione che abbiamo invece definito con un procedimento di diagonalizzazione, concettualmente analogo a quello con cui Georg Cantor dimostrò la non-numerabilità dell'insieme dei numeri reali.

Il lettore troverà una trattazione sistematica e rigorosa di questi argomenti in altri articoli dell'*Enciclopedia*. Qui vogliamo solo mostrare, con pochi accenni schematici, come queste considerazioni astratte permettano di capire piú a fondo problemi matematici classici. Molti di essi sono da tempo senza soluzione, nonostante gli intensi sforzi fatti per venirne a capo. Intuitivamente non è facile trovare ricette per dimostrare o refutare una congettura matematica. Non è facile, cioè, trovare un procedimento di decisione. Questa sensazione, vaga e generica, può venir rigorizzata esplicando come nel § 5.2 il concetto di computabilità e conseguentemente quello di decidibilità.

Facciamo subito un esempio. Se $P(a_1, ..., a_k, z_1, ..., z_n)$ è un polinomio a coefficienti interi nelle variabili $a_1, ..., a_k, z_1, ..., z_n$ l'equazione diofantea

$$(1) \qquad P(a_1, ..., a_k, z_1, ..., z_n)=0$$

permette di definire l'insieme delle k-ple $\langle a_1, ..., a_k \rangle$ di $\mathbf{N}^k$ tali che (1) ammette una soluzione nei numeri naturali $z_1, ..., z_n$ (in questo caso $a_1, ..., a_k$ sono i parametri dell'equazione). Un insieme cosí definito è detto diofanteo.

Matijasevič ha dimostrato nel 1970 che un insieme $S \subseteq \mathbf{N}^k$ è diofanteo se e solo se è ricorsivamente enumerabile (e cioè è vuoto oppure è il codominio di una k-pla di funzioni ricorsive primitive di una variabile).

Un risultato fondamentale nella teoria degli algoritmi assicura peraltro l'esistenza di un insieme ricorsivamente enumerabile $K \subset \mathbf{N}$ che non è ricorsivo (o Turing-computabile). Si può quindi trovare una equazione diofantea ad un parametro $P(a, z_1, ..., z_n)=0$ (quella che definisce K) per la quale non esiste alcun algoritmo in grado di deciderne la risolubilità in $z_1, ..., z_n$ per valori assegnati del parametro a. In questo modo Matijasevič è venuto a capo, dandone una risposta negativa, del X problema di Hilbert. Tale risposta negativa, come sempre nella storia della matematica, ha in realtà aperto molte nuove questioni ed ha gettato nuova luce su problemi classici della teoria dei numeri [cfr. Browder 1976, pp. 35-36 e anche pp. 323 sgg.].

Possiamo accennare solo brevemente a tutta una vasta gamma di altri risultati di indecidibilità (varie teorie algebriche, teorie assiomatiche dei numeri naturali, teorie assiomatiche dei numeri reali, logica dei predicati, problemi della parola per gruppi e semigruppi, ecc.). Per quanto riguarda invece problemi della decisione in senso stretto non solo richiamiamo brevemente il fatto che il calcolo booleano e corrispondentemente il calcolo proposizionale sono ovviamente decidibili (cfr. § 2.7), ma ricordiamo in particolare un risultato del 1960 di Richard Buchi, il quale ha mostrato che è decidibile l'aritmetica del secondo ordine debole a un posto, la teoria cioè che permette di trattare in modo duttile gli automi finiti (cfr. § 2.8).

6. *Complessità computazionale.*

6.1. Analisi «metanumerica».

Come l'indagine generale sulle proprietà logiche delle teorie si indica col nome di *meta*matematica, almeno dagli anni '30, cosí la riflessione sui problemi computazionali può venir designata come «analisi *meta*numerica». Già le considerazioni del § 5 si collocavano a un livello del genere, trattandosi di un'esplicazione della nozione «intrinseca» di computabilità perseguita nel contesto della teoria della Turing-computabilità o equivalentemente della teoria della ricorsività. Orbene, se in certe situazioni non pare necessario che la ricostruzione a livello di analisi metanumerica del procedimento di calcolo debba tener rigidamente conto degli algoritmi reali e soprattutto degli strumenti di calcolo, un modello adeguato può essere appunto una macchina di Turing o un algoritmo di Markov, resta il fatto che tali idealizzazioni «sembrano modelli abbastanza "poveri" di un Ibm 370 se appena vogliamo studiare problemi come la determinazione del valore di un polinomio» [Borodin e Munro 1975, p. 2]: per le considerazioni metanumeriche si aprono quindi altre direzioni di ricerca.

Analizziamo piú da vicino questo riferimento, tanto piú significativo in quanto i polinomi rappresentano, per cosí dire, un ponte tra analisi e algebra

e quindi sotto il profilo pratico il calcolo numerico di una funzione viene spesso sostituito dal calcolo di un polinomio che l'approssimi abbastanza bene, come abbiamo accennato nel § 4. Supponiamo di dover calcolare il valore del polinomio $P(x)=a_nx^n+\ldots+a_1x+a_0$ in un punto $x=x_0$. Invece di procedere nel modo tradizionale, possiamo scrivere $P(x)$ nella forma

$$(\ldots((a_nx+a_{n-1})x+a_{n-2})x+\ldots+a_1)x+a_0$$

nota usualmente come schema di Horner e utilizzare l'algoritmo che tale forma suggerisce. Cosa abbiamo guadagnato? Lo schema di Horner richiede n moltiplicazioni e n addizioni, ma dispensa da $n-1$ moltiplicazioni necessarie per calcolare $P(x)$ coll'algoritmo tradizionale.

È allora tipico dell'atteggiamento metanumerico chiedersi se lo schema di Horner sia «il miglior metodo possibile» rispetto al numero delle operazioni elementari richieste (nella fattispecie il problema, posto da Ostrowski (1954), è stato risolto affermativamente da Pan (1966)) e proprio problemi del genere giustificano la terminologia qui impiegata. «Il nome "analisi metanumerica" sembra appropriato non solo perché indica bene gli argomenti, cioè la metodologia del calcolo [*computation*], ma anche per il fatto che ha una relazione con il calcolo abbastanza analoga a quella della metamatematica con la matematica. In tale contesto affrontiamo problemi che riguardano particolari sistemi di dimostrazione, come l'esistenza di una dimostrazione di una certa forma o l'adeguatezza di un sistema in un dato contesto, ma incontriamo anche problemi che hanno a che fare con la dimostrabilità in generale senza riferirsi però a un particolare sistema di dimostrazione. Pensiamo, per esempio, all'indecidibilità di teorie matematiche [cfr. § 5.3]. Nell'analisi metanumerica analogamente non solo incontriamo problemi che concernono specifici sistemi di calcolo o certi tipi di macchine da calcolo, ma anche problemi come quello prima ricordato, che, pur avendo a che fare con il calcolo, sono indipendenti da ogni particolare metodo computazionale» [Cobham 1965, pp. 24-25].

Come l'analisi numerica ha una storia molto piú antica del termine che la designa (cfr. § 4.4), cosí l'ordine di idee che abbiamo qui brevemente delineato ed esemplificato ha i suoi autorevoli precedenti nella riflessione sulla bontà dei metodi computazionali via via proposti a partire da approcci ormai «classici», come in Newton e in Gauss; tuttavia l'aspetto istituzionale è ben piú recente, poiché finora si è soprattutto presa in considerazione la complessità computazionale dei problemi aritmetici e algebrici, in cui rientra tra l'altro la questione della procedura ottimale ricordata sopra per determinare i valori di un polinomio.

6.2. Complessità computazionale aritmetica e algebrica: un esempio.

Detto in breve – e in generale – la complessità computazionale è «lo studio di "ciò che rende le funzioni difficili da computare"» [Borodin e Munro 1975, p. 1]: l'accenno alle questioni specifiche che uno studio del genere comporta si presenta qui non solo come un naturale completamento di quel che abbiamo

detto nel § 5 sulla computabilità o come un particolare «metadiscorso» inerente alle procedure effettive di cui si è trattato nel § 4, ma permette di approfondire quelle stesse accezioni di «calcolo» che sono state delineate nei primi tre paragrafi.

Sono ricerche che come disciplina autonoma, dotata di una propria terminologia specifica, si sono definite solo negli anni '60: dopo lavori per certi aspetti pionieristici, come quello di Ostrowski (1954), una svolta in questa direzione è stata segnata da Vinograd [1967] che mirava a dare un quadro già abbastanza sistematico delle questioni inerenti alla determinazione del numero di moltiplicazioni necessarie per calcolare delle applicazioni da **N** in **N**. L'idea di fondo può essere schematizzata, rozzamente ma efficacemente, come un'esplicitazione della «impressione, difficile da digerire, che sotto il profilo computazionale le cose stiano diversamente per l'addizione che per la moltiplicazione» [Cobham 1965, p. 24; cfr. Knuth 1969, cap. IV].

Un esempio permette al solito di chiarire: nell'algebra lineare, come abbiamo già avuto modo di accennare marginalmente, non è che manchino classiche formule risolutive dei problemi. Nell'approccio formale tali questioni appaiono chiuse dopo la sistemazione ottocentesca: l'algebra lineare appare oggi piú uno strumento ausiliare di notevole importanza che una zona di frontiera nella ricerca. Non c'è nessuna difficoltà teorica, poniamo, nella risoluzione di un sistema di n equazioni in n incognite, proprio come, in via di principio, nulla ci impedisce di cercare gli autovalori di una matrice scrivendone l'equazione caratteristica e cercandone le radici.

Naturalmente, nella pratica, tutto ciò appare molto «etereo»: per risolvere un sistema di n incognite sviluppando direttamente gli opportuni determinanti si richiedono $n!n$ operazioni aritmetiche: siamo ben oltre la capacità di qualunque automa oggi realizzato. Ma non dobbiamo nutrire «illecite» speranze nemmeno per la tecnologia di domani. Per convenirne, basta un piccolo esperimento mentale: supponiamo di utilizzare un dispositivo di volume di lato V e composto di elementi ciascuno dei quali occupa un cubo D e prendiamo come velocità di trasmissione dell'informazione addirittura la velocità della luce $c=3\cdot10^8$ m/s, sicché il tempo necessario a un qualsiasi elemento per effettuare un'operazione elementare è almeno D/c. Ora maggioriamo con Vc/D^4 il numero totale di operazioni elementari eseguibile in un secondo dalla macchina e pensiamo ad un dispositivo enorme e composto da un numero altissimo di piccolissimi elementi, ponendo per esempio $V=1$ km³ e $D=10^{-8}$ cm, ordine di grandezza del raggio atomico; la nostra stima dà un numero grande, nel caso $1\cdot10^{57}$. Ma non «abbastanza» grande se abbiamo a che fare – come si è anticipato nel § 4.4 – con un sistema a un centinaio di incognite, per cui è $100!\simeq10^{157,9}$... Nemmeno il nostro gigantesco dispositivo avrebbe la capacità sufficiente per un calcolo del genere.

Inoltre i metodi classici appaiono non-adeguati anche per n relativamente piccolo, poniamo $n=20$, a causa degli errori di arrotondamento. Occorrono quindi dei trattamenti differenti, che si rivelano piú o meno vantaggiosi a seconda del numero di incognite, o dell'ordine, o del tipo della matrice qua-

drata del sistema preso in considerazione, ecc. Tale classificazione non è peraltro rigida, ma va di continuo rivista alla luce della riduzione del volume, dell'aumento della rapidità di funzionamento, ecc., delle varie modificazioni, insomma, dei dispositivi di calcolo.

Ciò premesso, limitiamoci a un problema particolare, quello del sistema lineare

$$\begin{cases} x' = ax + by \\ y' = cx + dy \end{cases}$$

Denotiamo al solito con $\mathbf{x} = \langle x, y \rangle$ il vettore delle incognite e con $\mathbf{x}' = \langle x', y' \rangle$ il vettore dei termini noti: lo specchio

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

formato dai quattro numeri a, b, c, d, rappresenta al solito la matrice associata al sistema, che riscriviamo compattamente

(1) $\mathbf{x}' = S\mathbf{x}$;

sotto l'ipotesi che S sia non-singolare, che cioè il suo determinante non sia nullo, è possibile determinare la matrice S^{-1} tale che

(2) $\mathbf{x} = S^{-1}\mathbf{x}'$.

Il problema di determinare le soluzioni $\mathbf{x}$ di (1) dato $\mathbf{x}'$ si riduce allora al problema di invertire la matrice S, cioè di determinare S^{-1}. Un possibile metodo consta dei due passi seguenti: 1) riduciamo la determinazione di S^{-1} a una moltiplicazione di matrici; 2) diamo un algoritmo per eseguire tale operazione.

Prescindiamo ora dal primo passo e concentriamoci sul secondo. L'algoritmo usuale per la moltiplicazione di due matrici quadrate di ordine n richiede n^3 moltiplicazioni e $n^3 - n^2$ addizioni. A prima vista sembra senza speranza il tentativo di ridurre il numero delle operazioni richieste. Per $n = 2$ esiste però un importante risultato di Strassen [1969]: questi presenta infatti un algoritmo che richiede 7 e non 8 moltiplicazioni. Posto

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \qquad AB = C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

possiamo allora calcolare C con la seguenza di operazioni

$$\begin{aligned} P_1 &= (a_{11} + a_{22})(b_{11} + b_{22}) \\ P_2 &= (a_{21} + a_{22})\, b_{11} \\ P_3 &= a_{11}(b_{12} - b_{22}) \\ P_4 &= a_{22}(-b_{11} + b_{21}) \\ P_5 &= (a_{11} + a_{12})\, b_{22} \\ P_6 &= (-a_{11} + a_{21})(b_{11} + b_{12}) \\ P_7 &= (a_{12} - a_{22})(b_{21} + b_{22}) \end{aligned}$$

$$\begin{aligned} c_{11} &= P_1 + P_4 - P_5 + P_7 \\ c_{12} &= P_3 + P_5 \\ c_{21} &= P_2 + P_4 \\ c_{22} &= P_1 + P_3 - P_2 + P_6. \end{aligned}$$

Un primo bilancio: abbiamo risparmiato 1 moltiplicazione, ma abbiamo in piú 14 addizioni, dato che l'algoritmo di Strassen ne impiega complessivamente 18, mentre quello usuale 4. Piú che «importante», come pure l'abbiamo definita, l'idea sembra a prima vista futile. Ma l'intuizione può sbagliare. Riflettiamo per un attimo alle proprietà formali del calcolo delle matrici: quel che aveva già colpito gli algebristi inglesi dell'Ottocento, come Cayley e Sylvester, era stato il fatto che per questo calcolo non valeva la regola commutativa. Orbene, il punto di forza dell'algoritmo di Strassen è che la proprietà commutativa della moltiplicazione non viene mai sfruttata. Gli elementi di A e di B sono usuali numeri: ma perché non generalizzare? Sostituiamo a tali numeri delle matrici, in modo da definire per induzione un opportuno algoritmo. Matrici di ordine 2^0 possono venir moltiplicate in 1 moltiplicazione, ovviamente. Matrici quadrate di ordine 2^{k+1} possono venir moltiplicate in 7 moltiplicazioni di matrici di ordine 2^k (e in 18 addizioni di matrici). $M(n)$ denoti allora il numero di moltiplicazioni che l'algoritmo usa per moltiplicare due matrici di ordine n (se n non è una potenza di 2, basta «completare» con degli 0 le matrici in modo che prendano questa forma).

Abbiamo allora

$$M(1) = 1 \qquad M(2^{k+1}) = 7M(2^k)$$

da cui si ha subito $M(2^k) = 7^k$. Posto $n = 2^k$ e scrivendo $\log a$ per indicare il logaritmo di a in base 2 otteniamo $M(n) = n^{\log 7}$ ove $\log 7$ ha il valore approssimato 2,81. Se n non è una potenza di 2, l'algoritmo richiede *al piú* $m = 7n^{2,81}$ moltiplicazioni. Un risultato buono? Per n abbastanza grande m è notevolmente minore di n^3, il numero delle moltiplicazioni richieste dall'algoritmo standard. E le addizioni? Strassen [1969] mostra che sono limitate da una costante moltiplicata per $n^{\log 7}$.

Ritorneremo sull'algoritmo di Strassen tra poche pagine. Per ora passiamo al primo passo, che momentaneamente avevamo lasciato da parte. L'idea di fondo si deve ancora a Strassen [1969]. Poniamo

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} I & 0 \\ ca^{-1} & I \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & h \end{pmatrix} \begin{pmatrix} I & a^{-1}b \\ 0 & I \end{pmatrix}$$

ove $h = a - ca^{-1}b$. Allora possiamo calcolare

$$S^{-1} = \begin{pmatrix} I & -a^{-1}b \\ 0 & I \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & h^{-1} \end{pmatrix} \begin{pmatrix} I & 0 \\ -ca^{-1} & I \end{pmatrix}$$

e abbiamo risolto il problema di invertire la matrice S (e di conseguenza anche il problema (1)). Anche in questo caso non si applica la regola commutativa del prodotto: per induzione si può quindi definire un algoritmo generale per matrici di ordine n. Sarà istruttivo segnalare una limitazione: nei passi intermedi l'algoritmo richiede che un certo numero di matrici piú piccole vengano invertite e alcune di esse potrebbero essere singolari anche se la matrice originale non lo è: in questo caso l'algoritmo si blocca. Ma ci sono sofisticazioni di questo algoritmo in cui l'ostacolo è aggirato [Borodin e Munro 1975, pp. 50 sgg.].

Ricerche come quelle cui abbiamo fatto cenno tendono, ancora, piú a chiarificare teoricamente la pratica del calcolo che di fatto a potenziarla. Il metodo di Strassen per la moltiplicazione di matrici può venir ulteriormente perfezionato (per esempio Vinograd nel 1971 ha ridotto a 15 il numero delle addizioni dell'algoritmo base). Non trattiamo qui le ragioni [Borodin e Munro 1975, p. 5] per le quali in molti casi l'algoritmo di Strassen risulta poco produttivo sotto il profilo dell'applicazione immediata: basti pensare che con una matrice di ordine n con $2^k < n < 2^{k+1}$ l'espediente di completare con degli 0 può rivelarsi sul piano pratico un vero impiccio per k abbastanza grande (secondo la tabella di p. 422). In un certo qual senso il metodo di Strassen è ancora notevolmente astratto: il suo interesse, peraltro, si coglie proprio a questo livello, nella acquisizione notevolmente profonda che la moltiplicazione di matrici non è un processo che richiede n^3 operazioni, contrariamente ad aspettative che paiono naturali a chi guarda esclusivamente all'algoritmo standard. Queste considerazioni ci portano naturalmente ai problemi dell'algoritmo ottimale. Una gamma di domande, ancora senza risposta: qual è il numero minimo di operazioni elementari richiesto per la moltiplicazione di due matrici di ordine n? È n^2, $n^2 \log n$ o proprio $n^{\log 7}$? Come trovare un algoritmo del genere? E come dimostrare che è ottimale?

La ricchezza di problemi aperti è segno della vitalità di una disciplina matematica. Il punto di vista maggiorare/minorare che abbiamo qui ritrovato sottende cosí notevoli approfondimenti di un ordine di idee che nelle sue componenti essenziali risale alle pratiche computistiche della tradizione aritmetica e algebrica che abbiamo delineato nel § 2. Il ben piú recente articolarsi del punto di vista «metanumerico» (anche in contesti piú sofisticati dell'algebra lineare, come quello degli elementi finiti nel § 4.7) secondo modalità che non hanno ancora assunto il carattere cumulativo e sistematico di altre regioni del sapere matematico ma hanno assunto il carattere di tentativi è un passaggio obbligato, che riproduce in questo settore una dinamica che altri aspetti del calcolo hanno già conosciuto. Boole [1854] lo diceva a suo tempo delle versioni piú astratte delle regole di calcolo guardando alla determinazione delle piú generali «leggi del pensiero»; possiamo parafrasarlo a proposito anche delle nostre analisi della calcolabilità e della difficoltà di calcolo delle funzioni. «Come i regni del giorno e della notte non sono nettamente delimitati, ma sono separati da una zona crepuscolare nella quale la luce dell'uno sfuma gradualmente nell'oscurità dell'altro, cosí possiamo dire che ogni regione della conoscenza positiva è circondata da un territorio in cui hanno libero campo la disputa e la speculazione

e sul quale la conoscenza positiva fa sentire la propria influenza e diffonde la propria luce in maniera piú o meno grande» [Boole 1854, trad. it. p. 547]. Ma «è importante qui come ovunque togliere alla scienza il velo del mistero» [Marx 1870-80, trad. it. p. 153].

7. *Conclusione.*

La battuta di Marx con cui abbiamo chiuso il § 6 si riferiva a quella fase dello sviluppo del calcolo differenziale in cui si passa dalla concezione di dy/dx come rapporto di quantità evanescenti a quello di «*espressione simbolica*, che indica quali operazioni dobbiamo eseguire con $f(x)$ per ottenere il valore effettivo di dy/dx, cioè $f'(x)$» [Marx 1870-80, trad. it. p. 80]. Nei *Manoscritti matematici* marxiani l'approccio di Lagrange, a un tempo operativo e algebrico, doveva segnare l'inizio della fase rigorosa destinata a liquidare quei «presupposti metafisici celati o palesi che a loro volta portano a conseguenze di ordine metafisico» [*ibid.*, p. 107], anche se non tutti gli assunti del genere erano individuati come tali, discussi e superati da Lagrange (del resto questi – osserva ancora Marx – segue in modo diretto il teorema di Taylor nella sua teoria delle funzioni derivate: altrettanto direttamente «Fichte seguí Kant, Schelling seguí Fichte, Hegel seguí Schelling, senza che né Fichte, né Schelling, né Hegel avessero discusso la base generale di Kant, cioè l'idealismo; altrimenti non avrebbero potuto continuare a svilupparlo» [*ibid.*, p. 164].

Non entriamo nel merito del giudizio di Marx come giudizio storico sul contributo lagrangiano; ci limitiamo invece a riflettere sul tipo di dialettica che cosí si individua. La constatazione della razionalità insita nell'atteggiamento di chi non mette in discussione le basi di un paradigma per poterne invece sviluppare le piú feconde direttive di ricerca fino ad esaurirle ci riporta all'antitesi arte/scienza nel contesto del calcolo, che implicitamente abbiamo già incontrato nei paragrafi precedenti.

Naturalmente il calcolo differenziale – come abbiamo accennato nel § 3 – ha lasciato ormai alle spalle l'epoca pionieristica in cui la parola 'arte' pareva piú adatta di 'scienza' per denotare un complesso di tecniche disparate, di espedienti ingegnosi ma non rigorosi, di metafisiche rivali, di crescita della conoscenza su fondamenti contraddittori. Il tempo in cui il vescovo Berkeley poteva rinfacciare in *The Analyst* (1734) che era piú oscuro un solo calcolo fatto dagli analisti newtoniani che non l'intera teologia razionale ci appare estremamente remoto.

Ma per altri aspetti del calcolo (o dei calcoli, cfr. § 1) le cose non stanno cosí: come abbiamo visto nei §§ 4, 5 e 6, certe tematiche di fondo dell'analisi numerica, dell'esplicazione del concetto di computabilità, della complessità computazionale rispettivamente sono ricche di situazioni ben diverse da quella ideale in cui un paradigma è in grado di individuare in modo univoco quali sono i problemi e che tipo di soluzioni ci aspettiamo. Per quanto concerne la nozione di computabilità e la complessità computazionale riteniamo che bastino come esem-

plificazioni quanto abbiamo detto nel § 5 sulla tesi di Church, sulla ricorsività e sulla sottoricorsività e, rispettivamente, la stessa conclusione del § 6. Riprendiamo invece in considerazione l'analisi numerica.

«La contrapposizione arte/scienza [in questo contesto] è dovuta a una sorta di principio d'indeterminazione, in cui spesso ci imbattiamo nel risolvere i problemi, il fatto cioè che determinare il modo migliore per risolvere un problema può richiedere la soluzione del problema stesso» [Ralston 1965, p. 1]. Non meno intricata è la situazione in cui il modo migliore di risolvere un problema dipende dalla conoscenza delle proprietà delle funzioni che vengono utilizzate, funzioni che spesso risultano non-ottenibili sia dal punto di vista teorico che da quello pratico (un caso del genere abbiamo segnalato, per esempio, nel § 4.8 trattando del metodo degli elementi finiti [cfr. anche *ibid.*, pp. 1-2 e *passim*]). E dunque: «*Come scienza* l'analisi numerica ha a che fare con quei procedimenti mediante i quali i problemi matematici possono venir risolti dalle operazioni aritmetiche. Ciò potrà talora richiedere lo sviluppo di algoritmi per risolvere problemi formulati già in un modo in cui le soluzioni possono venir trovate con mezzi aritmetici (per esempio sistemi di equazioni lineari: cfr. § 4.4 e anche § 6); ma qualche volta capiterà di dover sostituire quantità che non possono venir calcolate in modo aritmetico (per esempio derivate e integrali) con approssimazioni che ci permettono solo di trovare una soluzione approssimata. In quest'ultimo caso dovremo necessariamente prendere in considerazione gli errori che nel corso dell'approssimazione abbiamo commesso. Ma in entrambi i casi gli strumenti che impieghiamo nello sviluppo delle procedure dell'analisi numerica restano strumenti dell'analisi matematica esatta in senso classico. *Come arte* l'analisi numerica ha a che fare con la scelta di quella procedura che risulta ottimale nell'applicazione alla ricerca della soluzione di un dato problema. Ne consegue che chiunque impiega il calcolo numerico deve avere esperienza e, possibilmente, anche intuizione» [*ibid.*, p. 2].

Tutto ciò comporta una revisione di quel che usualmente intendiamo per «scoperta matematica»: il matematico, si chiedeva per esempio Hadamard [1945; in particolare l'introduzione] «scopre» o «inventa»? È paragonabile a Cristoforo Colombo che trova un nuovo continente o a Benjamin Franklin che escogita il parafulmine? I calcolatori ultraveloci non solo hanno profondamente mutato l'analisi numerica, aprendo nuovi problemi ma anche ristabilendo paradigmi che potevano parere desueti (cfr. quanto abbiamo detto nel § 4, in particolare di Fourier), ma hanno permesso di affrontare in un modo notevolmente diverso classici rompicapo che non rientrano immediatamente nelle questioni usualmente affrontate dai professionisti dell'analisi numerica. Non è difficile esemplificare. «Molti dei classici teoremi importanti nella teoria dei numeri furono scoperti come sottoprodotto della preparazione e dell'esame di tavole. Queste ultime erano costruite a mano. Le macchine moderne possono produrre tavole con velocità e precisione superiore di molti ordini di grandezza a quanto è umanamente possibile. Non solo la pubblicazione di tali tavole è impossibile ma anche il loro esame è spesso di gran lunga superiore alle possibilità umane. Diviene quindi evidente che dovrebbe essere compito della macchina

eseguire tale esame, ovviamente con un piccolo giudizioso aiuto del programmatore» [Lehmer 1969, p. 118]. Una rassegna di applicazioni alla teoria dei numeri si trova in Atkin e Birch 1971. Altre branche della matematica hanno conosciuto fenomeni analoghi: per esempio si dànno congetture di tipo geometrico nate dalla evidenza numerica e inimmaginabili a priori, cioè senza calcolo (è il caso della cosiddetta congettura di Birch e Swinnerton-Dyer [1965]).

Accenniamo a uno dei piú celebri rompicapo della topologia combinatoria, la congettura dei quattro colori, secondo cui quattro soli colori sono sufficienti per colorare una carta geografica nel piano (o sulla sfera) in modo che regioni contigue abbiano colori diversi. Questa congettura (che già aveva messo alla prova nell'Ottocento matematici come Moebius e Cayley) ha eluso i tentativi diretti via via elaborati ed è stata risolta in senso affermativo solo nel 1976 da tre matematici, Appel, Haken e Koch, che hanno utilizzato per un tempo considerevole un potentissimo calcolatore elettronico.

L'esempio dei quattro colori è per noi doppiamente interessante. In primo luogo ci permette di indicare un nuovo settore applicativo, ben diverso dall'area da cui abbiamo tratto la maggior parte degli esempi dei §§ 3 e 4 (l'area cioè che una volta veniva etichettata come «meccanica razionale» o «meccanica analitica» e cioè: meccanica del continuo, ottica, teoria dell'elasticità, ecc.): il settore di ricerca che grosso modo concentra la sua attenzione su collezioni di oggetti a carattere discreto, i quali agiscono in combinazione, un passo per volta.

In secondo luogo rappresenta un tipico caso di un problema il cui enunciato è ingannevolmente semplice, com'è del resto per molti altri rompicapo affrontati dall'analisi combinatoria. Può parere forse paradossale il fatto che, dopo secoli di polemica sulla liceità dell'infinito matematico, siano le collezioni finite a rivelarsi gli oggetti di studio piú difficili. Nei successi e nelle speranze che offrono oggi i calcolatori in settori del genere possiamo ritrovare ancora le antitesi astratto/concreto, procedimento meccanico / procedimento creativo, ecc. che già ci hanno fornito dei riferimenti nel corso dei paragrafi precedenti. Con tutta la sua complessità come macchina, il calcolatore elettronico serve a semplificare problemi che altrimenti sembrano soverchiare l'intelletto umano. Ha dunque lo stesso scopo della matematica tradizionale, ma delle modalità di comportamento differenti. All'invenzione ardita e geniale sostituisce una procedura di ricerca-scoperta, per cosí dire, a setaccio. «Si tratta di uno sforzo coordinato uomo-macchina nel quale l'uomo fornisce la migliore informazione che possiede sul tipo di dimostrazione che ha piú probabilità di successo e la macchina tenta di eseguire tutte le tappe in modo esaustivo» [Lehmer 1969, p. 119].

Tale aspetto non dev'essere tuttavia estremizzato: l'approccio calcolistico ai problemi (per esempio combinatori, di teoria dei numeri, geometrici, ecc.) non è di per sé riduttivo del carattere astratto della ricerca matematica: nel senso che abbiamo chiarito nei paragrafi precedenti, aritmetica e logica booleana costituiscono infatti i riflessi fondamentali dell'elaboratore ed è questo il motivo per cui appare lecito asserire che l'elaboratore possiede una capacità intrinseca di manipolare concetti astratti. Il fatto che in questo ordine di idee

si siano escogitati metodi con cui l'elaboratore può manipolare concetti molto generali, scoprire la dimostrazione di congetture generali e addirittura indirizzare le proprie esplorazioni concettuali in base a principî euristici di eleganza, efficacia, ecc. e che tuttavia l'indagine motivata dall'esplicazione del concetto intuitivo di calcolabilità metta in luce anche l'inadeguatezza di certi strumenti e di certe strategie per particolari problemi o per classi di problemi ripropone a un nuovo livello le dicotomie scoprire/inventare, arte/scienza, ecc. da cui in questo paragrafo abbiamo preso le mosse.

Potremmo quindi terminare indicando in quest'ultima chiave di lettura una (non certo l'unica) possibilità di ritrovare un'unità concettuale sottostante alle svariate accezioni di 'calcolo'. Ma siamo debitori di una confessione al lettore che ci ha seguito fin qui: Joyce definiva il resoconto delle peregrinazioni dublinesi di Ulisse-Bloom «una cronaca omnicomprensiva, micraniosa e farraginosissima». La nostra invece può aspirare solo alle ultime due qualifiche. Gli sviluppi dei calcoli algebrici e logici, l'analisi reale e soprattutto quella complessa, l'estensione del calcolo alle varietà, la teoria generale delle equazioni differenziali, la teoria delle distribuzioni, ecc. ben altro spazio avrebbero meritato e l'elenco di quel che *non* c'è potrebbe continuare ancora. Valgano, a parziale scusante, quei riferimenti e accenni che nei vari paragrafi possono suggerire un aggancio ad altre voci dell'*Enciclopedia*.

Si diceva nel § 1 della difficoltà di orientare il lettore nelle ramificazioni che, in contesti sempre piú specialistici, ha l'idea di calcolo. La specializzazione è il prezzo che si paga per il rigore: l'abbandono della *foi du charbonnier* ha spesso come compagno l'aumento della complessità. Cosí non abbiamo nemmeno tentato di fornire al lettore una mappa del labirinto; abbiamo solo cercato di fargli intendere che si trova in un labirinto. [G. G. e G. G.].

Atkin, A. O., e Birch, B. J.
1971 (a cura di) *Computers in Number Theory*, Academic Press, New York.

Babuška, I., e Rheinboldt, W.
1977 *Computational Aspects of Finite Element Analysis*, in «Computer Science Technical Report Series», University of Maryland, College Park Md (ciclostilato).

Birch, B. J., e Swinnerton-Dyer, H. P. F.
1965 *Notes on Elliptic Curves, II*, in «Journal für die reine und angewandte Mathematik», CCXVIII, pp. 79-108.

Bocheński, J. M.
1956 *Formale Logik*, Alber, Freiburg-München (trad. it. Einaudi, Torino 1972).

Bombelli, R.
1579 *L'algebra*, Rossi, Bologna.

Boole, G.
1847 *The Mathematical Analysis of Logic, Being an Essay toward a Calculus of Deductive Reasoning*, Macmillan, Barclay and Macmillan, Cambridge (trad. it. Silva, Milano 1965).
1854 *An Investigation of the Laws of Thought, on which are Founded the Mathematical Theories of Logic and Probabilities*, Walton and Maberly, London (trad. it. Einaudi, Torino 1976).

Borodin, A., e Munro, I.
1975 *The Computational Complexity of Algebraic and Numeric Problems*, American Elsevier, New York.

Bourbaki, N.
1960 *Eléments d'histoire des mathématiques*, Hermann, Paris (trad. it. Feltrinelli, Milano 1963).

Braithwaite, R. B.
1953 *Scientific Explanation*, Cambridge University Press, London (trad. it. Feltrinelli, Milano 1966).

Browder, F.
1976 (a cura di) *Mathematical Developments Arising from Hilbert Problems*, American Mathematical Society, Providence R.I.

Carnap, R.
1939 *Foundations of Logic and Mathematics*, Chicago University Press, Chicago (trad. it. Paravia, Torino 1967²).
1942 *Studies in Semantics*, I. *Introduction to Semantics*, Harvard University Press, Cambridge Mass.

Carnot, L.-N.-M.
1797 *Réflections sur la métaphysique du calcul infinitésimal*, in *Œuvres mathématiques*, Decker, Basle.

Cauchy, A.-L.
1821 *Cours d'Analyse*, Imprimerie royale, Paris.
1840-47 *Exercices d'analyse et de physique mathématique*, 4 voll., Bachelier, Paris.

Ciarlet, P. G.
1978 *Numerical Analysis of the Finite Element Method for Elliptic Boundary Value Problems*, North-Holland, Amsterdam.

Cobham, A.
1965 *The Intrinsic Computational Difficulty of Functions*, in Y. Bar-Hillel (a cura di), *Logic, Methodology and Philosophy of Sciences*, North-Holland, Amsterdam, pp. 24-30.

Comte, A.
1830-42 *Cours de philosophie positive*, 6 voll., Rouen Frères (Bachelier), Paris (trad. it. parziale Radar, Padova 1967).

Courant, R., e Hilbert, D.
1962 *Methods of Mathematical Physics*, vol. II, Interscience and Wiley, New York - London.

Courant, R., e Robbins, H.
1941 *What is Mathematics?*, Oxford University Press, London - New York (trad. it. Boringhieri, Torino 1972²).

Dahlqvist, G.; Björck, A.; e Anderson, N.
1974 *Numerical Methods*, Prentice-Hall, Englewood Cliffs N.J.

De Morgan, A.
1847 *Formal Logic; or, the Calculus of Inference, Necessary and Probable*, Taylor and Walton, London.

Descartes, R.
1644 *Principia Philosophiae*, Elzevir, Amsterdam (trad. it. in *Opere*, Laterza, Bari 1967, vol. II).

Dieudonné, J.
1968 *Calcul infinitésimal*, Hermann, Paris.

Eulero, L.
1755 *Institutiones calculi differentialis cum eius usu in analysi finitorum ac doctrina serierum*, Impensis Academiae Imperialis Scientiarum Petropolitanae.
1768 *Institutionum calculi integralis volumen primum*, Impensis Academiae Imperialis Scientiarum, Petersburg.
1770 *Vollständige Anleitung zur Algebra*, Kayserliche Akademie der Wissenschaften, Sankt Petersburg.

Fermat, P. de
1670 *Diophanti... arithmeticarum libri sex... cum... observationibus P. de Fermat... Accessit doctrina analyticae inventum novum collectum*, s. e., Toulouse (trad. it. Boringhieri, Torino 1969).

Forsythe, G. E., e Moler, C. B.
1967 *Computer Solution of Linear Algebraic Systems*, Prentice-Hall, Englewood Cliffs N.J.

Fourier, J.-B.-J.
1822 *Théorie analytique de la chaleur*, Didot, Paris.

Frola, E., e Miranda, C.
1941 *Lezioni di geometria analitica e proiettiva*, Biamino, Torino.

Gauss, C. F.
1801 *Disquisitiones arithmeticae*, Fleischer, Leipzig.
1813 *Disquisitiones generales [circa seriem infinitam]... Pars prior*, Dieterich, Göttingen; ora in *Werke*, tomo III, Dieterich, Göttingen 1866.

Hadamard, J.
1945 *The Psychology of Invention in the Mathematical Field*, Princeton University Press, Princeton N.J.

Henrici, P.
1963 *Error Propagation for Difference Methods*, Wiley, New York.

Hilbert, D.
1900 *Mathematische Probleme. Vortrag, gehalten auf dem Internationalen Mathematiker Kongress zu Paris 1900*, in «Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse», pp. 253-97.

Huntington, E. V.
1904 *Sets of Independent Postulates for the Algebra of Logic*, in «Transactions of the American Mathematical Society», V, pp. 288-309.

Kneale, W. C., e Kneale, M.
1962 *The Development of Logic*, Clarendon Press, Oxford (trad. it. Einaudi, Torino 1972).

Knuth, D. E.
1965 *The Art of Computer Programming*, I. *Fundamental Algorithms*, Addison-Wesley, Reading Mass.
1969 *The Art of Computer Programming*, II. *Seminumerical Algorithms*, Addison-Wesley, Reading Mass.

Lakatos, I.
1970 *Falsification and the Methodology of Scientific Research Programs*, in I. Lakatos e A. M. Musgrave (a cura di), *Criticism and the Growth of Knowledge*, Cambridge University Press, London (trad. it. Feltrinelli, Milano 1976, pp. 164-276).

Laplace, P.-S. de
1814 *Essai philosophique sur les probabilités*, Courcier, Paris (trad. it. in *Opere*, Utet, Torino 1967).

Lehmer, D. H.
1969 *Computer Technology Applied to the Theory of Numbers*, in W. J. LeVeque (a cura di), *Studies in Number Theory*, The Mathematical Association of America, Prentice-Hall, Englewood Cliffs N.J., pp. 117-51.

Lichtenberg, G. F.
1844-47 *Vermischte Schriften*, 8 voll., Dieterich, Göttingen (trad. it. *Osservazioni e pensieri*, Einaudi, Torino 1966).

Mach, E.
1883 *Die Mechanik in ihrer Entwicklung historisch-kritisch dargestellt*, Brockhaus, Leipzig (trad. it. Boringhieri, Torino 1968).

Marx, K.
[1870-80] [I teoremi di Taylor e MacLaurin e la teoria delle funzioni di Lagrange] (trad. it. in *Manoscritti matematici*, Dedalo, Bari 1975).

Mendelson, E.
1964 *Introduction to Mathematical Logic*, Van Nostrand, Princeton N.J. (trad. it. Boringhieri, Torino 1972).
1970 *Boolean Algebras and Switching Circuits*, McGraw-Hill, New York (trad. it. Etas Kompass, Milano 1975).

Menger, K.
1945 *Methods of presenting e and π*, in «American Mathematical Monthly», LII, pp. 28-33.

Meschkowski, H.
1960 *Wandlungen des mathematischen Denkens*, Vieweg, Braunschweig 1960² (trad. it. Boringhieri, Torino 1973²).

Michel, P.-H.
1950 *De Pythagore à Euclide*, Belles Lettres, Paris.

Peano, G.
1898 *Formulaire de mathématiques*, II, § 2: *Arithmétique*, pubblicato dalla «Rivista di Matematica», Torino; ora in *Formulario mathematico*, Cremonese, Roma 1960.

Picutti, E.
1977 *Sul numero e la sua storia*, Feltrinelli, Milano.

Poincaré, H.
1902 *La science et l'hypothèse*, Flammarion, Paris (trad. it. Signorelli, Roma 1968²).
1908 *Science et méthode*, Flammarion, Paris.

Popper, K.
1959 *The Logic of Scientific Discovery*, Hutchinson, London (trad. it. Einaudi, Torino 1970).
1972 *Objective Knowledge, an Evolutionary Approach*, Clarendon Press, Oxford (trad. it. Armando, Roma 1975).

Preti, G.
1953 *Linguaggio comune e linguaggi scientifici*, pubblicazioni della «Rivista critica di storia della filosofia», n. 3, Bocca, Milano-Roma; ora in *Saggi filosofici*, La Nuova Italia, Firenze 1976, vol. I, pp. 127-220.

Ralston, A.
1965 *First Course in Numerical Analysis*, McGraw-Hill, New York.

Ritchie, R. W.
1963 *Classes of Predictably Computable Functions*, in «Transactions of the American Mathematical Society», CVI, pp. 139-73.

Russell, B.
1919 *Introduction to Mathematical Philosophy*, Allen and Unwin, London (trad. it. Longanesi, Milano 1947).

Russell, B., e Whitehead, A.
1910 *Principia mathematica*, Cambridge University Press, London.

Schwartz, L.
1966 *Théorie des distributions*, Hermann, Paris (1ª ed. in 2 voll. 1950-51).
1972 *La function δ et les noyaux*, in A. Salam e E. P. Wigner (a cura di), *Aspects of Quantum Mechanics*, Cambridge University Press, New York, pp. 179-82.

Shannon, C. E.
1953 *Computers and Automata*, in «Proceedings of the Institute of Radio Engineers», XLI, pp. 1234-41 (trad. it. in V. Somenzi (a cura di), *La filosofia degli automi*, Boringhieri, Torino 1965, pp. 93-115).

Strang, G., e Fix, G.
1973 *An Analysis of the Finite Element Method*, Prentice-Hall, Englewood Cliffs N.J.

Strassen, V.
1969 *Gaussian Elimination is not Optimal*, in «Numerische Mathematik», XIII, pp. 354-56.

Tartaglia, N.
1556 *General Trattato di numeri, et misure*, Troiano dei Navò, Venezia.

Turing, A. M.
1950 *Computing Machinery and Intelligence*, in «Mind», LIX, pp. 433-60 (trad. it. in V. Somenzi (a cura di), *La filosofia degli automi*, Boringhieri, Torino 1965, pp. 116-56).

Vinograd, S.
1967 *On the Number of Multiplications Required to Compute Certain Functions*, in «Proceedings of the National Academy of Sciences», LVIII, pp. 1840-42.

Waismann, F.
1936 *Einführung in das mathematische Denken*, Gerold, Wien (trad. it. Boringhieri, Torino 1965).

Whitehead, A. N.
1898 *A Treatise on Universal Algebras with Applications*, Cambridge University Press, London.

Il calcolo, sia quello con i numeri naturali (cfr. **numero**) – **zero** incluso – sia quello con le **funzioni**, sia il calcolo **differenziale** e **infinitesimale**, sia quello logico (cfr. **logica**) è al centro e della matematica «speculativa» (cfr. **matematiche**) e della **scienza** applicata. Infatti, nello studio dei modelli (cfr. **modello**) inerenti alla **fisica** (cfr. **sistema, energia**), alla biologia (cfr. **vita, gene**) o ai vari campi delle applicazioni tecniche, gli strumenti del calcolo esaminati nell'articolo che precede svolgono – insieme a quelli di **probabilità** e di **combinatoria** – un ruolo fondamentale anche nell'applicazione dei concetti astratti di **locale/globale**, **stabilità/instabilità**, **continuo/discreto**, **ricorsività**. La costruzione dei modelli rinvia naturalmente anche al calcolo numerico e quindi alla simulazione mediante opportuni **strumenti** (cfr. **macchina**, **analogico/digitale**, **automa**) dei fenomeni esaminati.

Numero

1. *'Uno' è un numero?*

Questa domanda suonerebbe perlomeno strana a qualsiasi principiante di matematica che abbia una minima dimestichezza con la successione infinita dei numeri «naturali» 1, 2, 3, ... Eppure nella matematica greca è abbastanza abituale imbattersi, dai pitagorici in poi, in affermazioni tipo «'Uno' non è un numero»; «'Uno' non è né pari né dispari», ecc. [cfr. Bourbaki 1960, trad. it. p. 149].

Affermazioni del genere sono oggi usualmente ritenute false, se non addirittura prive di senso. Ma per i Greci la cosa era diversa: «SOCRATE. ... Un uomo tale [il matematico] potrà mai da sé a sé fare calcoli di numeri che abbia solo nella mente; o farà altri calcoli di cose che sono fuori di lui, fra quante sono numerabili? TEETETO. E come no? SOCRATE. Ma fare un calcolo non è altro, diremo, che computare quanto un numero viene a essere» [Platone, *Teeteto*, 198c]. Dunque qui il termine ἀριθμός «indica in ogni caso *un numero definito di cose definite*... Quando Platone parla di numeri (*Repubblica*, 525d) che hanno "corpi visibili e tangibili", bisogna prenderlo pressoché alla lettera» [Klein 1934-36, ed. 1968 pp. 46-47]. Il detto «Ogni numero è numero di qualcosa» pare inoltre compendiare la stessa opinione di Aristotele, come chiarisce il commentatore Alessandro: πᾶς γὰρ ἀριθμός τινός ἐστι [Commento alla *Metafisica*, 86, 5].

La contrapposizione fra il greco ἀριθμός e il 'numero' attuale non è adeguatamente descrivibile come una particolare versione della contrapposizione concreto/astratto. Anche il numero «puro» cui si è oggi abituati (senza qualificazioni, cioè senza intendere «numero *di qualcosa*») può venir considerato tanto «concreto» quanto un dato numero di mele, bambini, pietruzze, ecc. Dopo tutto, pressoché cent'anni fa, il logico Gottlob Frege era solito dire che «il numero è una cosa...» Quel che caratterizza il «numero» dei Greci è, allora, «una doppia determinatezza; è, innanzitutto, e sempre, numero di oggetti *determinati in un dato modo* ed è, in secondo luogo, un'indicazione del fatto che ci sono *tanti* di quegli oggetti... Nel far di conto [cfr. il passo di Platone di cui sopra], nell'*actus exercitus* (per usare la terminologia scolastica) è solo *la molteplicità delle cose contate* oggetto di attenzione. Può venir "contato" solo ciò che è davanti a noi in un certo numero: né un oggetto percepibile dai sensi né *una* pura unità è *un numero* di cose o unità. L'"unità" come tale non è un ἀριθμός, un fatto che pare bizzarro solo se si presuppone la nozione della "successione dei numeri naturali"» [Klein 1934-36, ed. 1968 p. 49].

Ci sono ovviamente eccezioni a questo punto di vista. Ma queste *eccezioni* sono *infrazioni*. L'episodio [riportato e commentato in Heath 1921, I, p. 69] relativo a Crisippo di Soli (III secolo a. C.) che avrebbe parlato di una «moltitudine uno», è significativo. Giamblico, secoli piú tardi, lo rimprovera di palese assurdità; Heath ne valuta invece l'apporto come «tentativo di far entrare 1

nel concetto di numero» [*ibid.*]. La morale della storia è chiara: «Quel che Giamblico prendeva per una confusione, oggi noi lo teniamo per certo... La palese assurdità potrebbe rivelarsi una funzione della sottostante classificazione che vien data per scontata. La classificazione usuale dei numeri presso gli antichi Greci è chiaramente differente dalla nostra. Differenti risulteranno quindi le violazioni dell'ordine e della coerenza, differenti, di conseguenza, saranno le confusioni e le contraddizioni» [Bloor 1976, p. 98]. La ragione della differenza va cercata specificamente nella concezione dell'unità come ἀρχή 'principio' o 'fonte' dei numeri.

Ma l'infrazione è anche in grado di diventare nuova regola. Nella sua *Arithmétique* Simon Stevin, dopo aver detto che «l'aritmetica è la scienza dei numeri» [1585, p. 1*v*] e che «numero è ciò mediante cui si esplica la quantità di ogni cosa», aggiunge subito che «l'unité est nombre», 'uno' è un numero. Contro l'opinione di «vecchi e nuovi filosofi» [*ibid.*, p. 2*r*] dichiara di essere certo di tale tesi proprio «come se la Natura stessa me l'avesse detto di sua bocca». La contrapposta tesi circa l'uno come semplice «cominciamento» è completamente falsa: la parte – dice Stevin – è «della stessa materia» del tutto; l'unità è parte di una moltitudine di unità ma «la matière de multitude d'unitez est nombre», quindi «materia» dell'unità è il numero, ovvero l'unità è essa stessa un numero. Chi nega quest'ultimo passo si sentirebbe di negare che un pezzo di pane non sia ancora del pane? Stevin ha in questo modo fondato una nuova classificazione «naturale» [cfr. le osservazioni di Bloor 1976, pp. 103-5].

2. *La $\sqrt{2}$ e le metafisiche influenti.*

Leibniz soleva illustrare la distinzione fra verità necessarie e contingenti, fra grandezze commensurabili e incommensurabili con «un esempio tratto dalla geometria e dai numeri» [cfr. Grua 1948, I, p. 303]. Pur avendo anche una coppia di grandezze incommensurabili un determinato rapporto, l'esplicitazione numerica di questo comporta, come le verità contingenti, una sorta di procedura infinita, che solo Dio è capace di afferrare, in quanto penetra l'infinito con un'unica intuizione. E la metafora delle grandezze incommensurabili ricorre ancor oggi nella considerazione di «paradigmi» incommensurabili [cfr. Kuhn 1976, p. 191]. Del resto, si cita $\sqrt{2}$ in questa stessa *Enciclopedia* per piú aspetti: come esemplificazione del passaggio da algoritmi finiti a procedure infinite (cfr. l'articolo «Calcolo», vol. II, p. 415); come paradigma di modificazioni del pensiero matematico ostacolate dai residui di precedenti ontologie (cfr. «Conoscenza», vol. III, p. 787); come caso tipico dell'emergenza di nozioni implicite, favorita dal successo di tecniche di calcolo o di dimostrazione (cfr. «Deduzione/prova», vol. IV, p. 495); come slittamento sul piano del rigore (cfr. «Identità/differenza», vol. VI, pp. 1132-33); come spia di inadeguate modellizzazioni (cfr. «Modello», vol. IX, § 2), ecc. Si tratta quindi di un caso storico estremamente «pregnante» e per il pensiero matematico e per la stessa molteplicità conflittuale delle *filosofie*. In cosa sta il suo «fascino»? A nostro avviso, sostanzial-

mente nel fatto di essere legato, nella tradizione intellettuale occidentale, ad un *cambio di metafisica*.

Si riconsideri la tradizionale dimostrazione dell'irrazionalità di $\sqrt{2}$ (com'è riportata, per esempio, in «Calcolo», vol. II, p. 415). «A rigore, essa mostra solo che $\sqrt{2}$ *non* è numero razionale; ma per noi non c'è evidentemente altro significato: se $\sqrt{2}$ non è un numero razionale è certo *un numero* irrazionale. Ma non era questo che provava per i Greci. Per essi provava invece che $\sqrt{2}$ *non* era affatto *un numero*... Cosa davvero dimostra, allora, una tale dimostrazione? Che $\sqrt{2}$ è irrazionale o che non è un numero? La risposta dipende dalle assunzioni di sfondo circa il numero con le quali si considera lo stesso processo calcolistico» [Bloor 1976, p. 109]. L'idea di numero come aggregato di piccoli punti (come era sia nel pitagorismo sia nell'atomismo antico) è la «metafisica influente» (per questa terminologia, cfr. l'articolo «Metafisica», in questo stesso volume, p. 167), che permette di escludere $\sqrt{2}$ dai «numeri» (οὐκ ἐν ἀριθμοῖς; cfr. «Calcolo», vol. II, p. 415), metafisica differente dalla attuale che tranquillamente contempla la possibilità di assegnare a ogni punto della retta geometrica un «numero» (cfr. *ibid.*, p. 390).

Questa differenza non deve mettere in ombra il fatto che le due metafisiche – la greca e quella definitivamente impostasi con l'analisi ottocentesca del continuo – hanno pure elementi in comune. In entrambe, per esempio, i «numeri» per eccellenza, cioè i numeri naturali (o interi positivi), a parte il caso dell'unità (cfr. § 1), vengono ripartiti in «pari» e «dispari»; Bloor al proposito delinea allora il seguente esperimento mentale: «Immaginiamo una cultura in cui si siano apprese molte cose interessanti sui numeri, ma senza mai dare troppa importanza alle categorie di "pari" e "dispari"; in cui magari si sono anche utilizzate proprietà del genere, ma senza isolarle o dar loro troppo peso. I matematici di quella cultura non si sarebbero mai sognati di compilare una tavola delle opposizioni; al contrario dei pitagorici, si sarebbero limitati ad affiancare il pari e il dispari ad altre dicotomie cosmiche. Forse, al contrario che ai pitagorici, giorno e notte, buono e cattivo, bianco e nero, ecc. non sarebbero parsi loro degli opposti cosí irriducibili e ovvii. Dopo tutto, la notte sfuma nel giorno, il buono nel cattivo e il nero nel bianco... Una simile cosmologia sarebbe stata ancora intellegibile, e avrebbe potuto anzi essere notevolmente sofisticata. Il calcolo [su cui si regge la dimostrazione dell'irrazionalità di $\sqrt{2}$], interpretato come una dimostrazione che i numeri possono essere pari *e* dispari, non avrebbe creato problemi, anzi avrebbe ulteriormente confermato l'idea che rigidi confini non sono realistici» [1976, p. 110]. Forse Borges ha, in qualche sua favola, delineato i contorni di una civiltà dotata di una simile cultura matematica... Ma per i pitagorici, e per i Greci in genere, l'unico ente matematico *parimpari* era l'unità, che non è propriamente un «numero» (cfr. § 1); dunque la scoperta dell'irrazionalità di $\sqrt{2}$, cioè dell'incommensurabilità della diagonale e del lato del quadrato, cui presto dovevano affiancarsi altri problemi – come la duplicazione del cubo e la trisezione dell'angolo – tutti implicanti l'esistenza di irrazionali (per non dire di quello del rapporto fra la circonferenza e il diametro di un cerchio!), costituisce una genuina «crisi» proprio perché «suggerisce ai Greci una separazione tra grandezza e numero opposta alla loro precedente tendenza a immaginare linee, superfici, ecc. costituite di punti materiali... Ma [in una differente cosmologia] quel che fu una crisi sarebbe stata una semplice anomalia» [*ibid.*]. L'eco delle «metafisiche influenti» di Eudosso e di Platone, di Aristotele e di Euclide, ecc. perverrà fino alle teorie dei numeri reali di Weierstrass, Cantor, Dedekind, ecc. [per cui si veda, ad esempio, Kline 1972, pp. 982-87]: in tale contesto la dimostrazione classica potrà venire agevolmente e «rigorosamente» *re*interpretata come la dimostrazione che $\sqrt{2}$ è *un numero* irrazionale.

3. *Estensioni del dominio numerico.*

I due riorientamenti di cui si è detto, concernenti rispettivamente 1 e $\sqrt{2}$, rientrano a loro volta in un piú articolato processo incentrato sulla nozione di numero, che vede progressivamente l'estendersi del dominio numerico dai numeri naturali – fatte salve le obiezioni a considerare 1 un «numero» (cfr. § 1) – alle frazioni e agli interi relativi, per pervenire ai «numeri» reali e complessi. Questa dinamica complementare al rigore «geometrico» tipico della tradizione greca è stata una sorta di «pragmatismo matematico» [Bourbaki 1960, trad. it. p. 148] che sembra aver le sue radici nella straordinaria abilità calcolistica dei popoli del Vicino Oriente antico e poi di Indiani e Arabi: nell'articolo «Calcolo» di questa stessa *Enciclopedia* il lettore troverà delineati i tratti di questa «tensione essenziale» fra «tradizione e innovazione» (per dirla con Kuhn [1977]) che ha visto infine tramutare regole empiriche di calcolo in proprietà formali. Sarà qui presupposto quanto detto in quella sede, in particolare circa i sistemi **Z** e **Q** degli interi relativi e dei razionali (con segno), che si affiancano al sistema **N** dei naturali (potenziato dall'aggiunzione dello *zero*) e relativo apparato algebrico (cfr. «Calcolo», § 2), e circa la presentazione assiomatica dei numeri reali **R** e dei numeri complessi **C** come spazio normato su **R** (cfr. *ibid.*, § 3).

Locuzioni come quelle che si leggono nello straordinario latino di Newton o di Leibniz testimoniano delle difficoltà di questo processo in cui il concetto di numeri è stato sottoposto a una sorta di «tensione» [per la tensione dei concetti in matematica, si veda, in generale, Lakatos 1961-74] che ha permesso di ritrovare nei vari sistemi numerici via via prodotti una sorta, direbbe Wittgenstein, di «aria di famiglia»; ma al prezzo di violare «leggi dell'aritmetica» che in precedenza si riteneva esprimessero proprietà «essenziali» del «numero». Cosí Newton nella sua *Arithmetica universalis*: «Per numerum non tam multitudinem unitatum, quam abstractam quantitatis cuiusvis ad aliam eiusdem generis quantitatem, quae pro unitate habetur, rationem intelligimus. Estque triplex: Integer, Fractus et Surdus, Integer quem unitas metitur, Fractus quem unitatis pars submultiplex metitur, et Surdus cui unitas est incommensurabilis» («Per numero intendiamo non tanto una raccolta di piú unità, quanto il rapporto astratto di una quantità qualunque rispetto ad un'altra quantità dello stesso genere, che si considera come unità. Ed è di tre specie: intero, fratto e sordo. L'intero è misurato dall'unità, il fratto da un sottomultiplo dell'unità, sordo è

incommensurabile con l'unità») [1707, I, II, capov. III]. *Surdus*, ovviamente da *absurdus*. E Leibniz, a proposito dell'unità immaginaria, parla di «analyseos miraculum, idealis mundi monstrum, pene inter ens et non ens amphibium» («prodigio dell'analisi, mostro del mondo ideale, quasi anfibio tra ente e non ente») [1702]. Ed è proprio questo dispiegarsi del calcolo come una manipolazione di simboli secondo regole che hanno tramutato le «assurdità» e le «patologie», che emergono via via nella pratica del calcolo, in strumenti intellettuali atti a rimodellare i confini di quella stessa pratica. «Mostri», sí, ma «mostri promettenti» (*hopeful monsters*) [per questa terminologia, cfr. Lakatos 1961-74, trad. it. pp. 61 sgg.], che tale pratica sono destinati a rinnovare.

4. *Numeri primi e aritmetica moltiplicativa.*

4.1. Problemi aritmetici.

«Chi cerca dei metodi senza aver in testa un problema cerca, per la maggior parte del tempo, invano». È in quest'ottica che, al II Congresso internazionale dei matematici tenuto a Parigi nel 1900, Hilbert ha proposto i suoi celebri ventitré problemi la cui soluzione necessita nuovi metodi destinati a rivelarsi «importanti» nelle matematiche [Hilbert 1900, ed. 1976 p. 6]. Ma per utilizzare una distinzione su cui si articola la stessa *Enciclopedia*, se i metodi sono *im*portanti, i problemi, a loro volta, sono *portanti*. Costituiscono infatti la nervatura della ricerca: per dirla ancora con Hilbert, sia che si tratti – come nel caso del problema relativo alla congettura di Fermat – di «libera invenzione della ragione pura», sia che vengano motivati dalla «necessità di comprendere i piú semplici fenomeni naturali» [*ibid.*, p. 2], essi costituiscono un «ponte» fra discipline i cui specialisti, altrimenti, «faticherebbero a intendersi» [*ibid.*, p. 34]: «sentieri che guidano in un labirinto di verità nascoste» [*ibid.*, p. 2]. Ma garanti cosí dell'unità «profonda» delle matematiche, i problemi debbono entrare, per ciò stesso, nello specifico della ricerca. Pur riconoscendo, e trattando ampiamente [cfr. *ibid.*, problemi I-VI], «il fascino dei fondamenti», Hilbert è infatti convinto che «per penetrare nel regno della scienza è indispensabile occuparsi anche di problemi particolari» [*ibid.*, p. 15], come già Weierstrass aveva a suo tempo ammonito. Ovvero «solo l'architetto che conosce a fondo, in tutti i dettagli, le diverse funzioni dell'edificio, sarà in grado di porne in piena sicurezza le fondamenta» [*ibid.*].

Dunque non basta una qualche fondazione (assiomatica: cfr. gli assiomi di Peano riportati nel già citato articolo «Calcolo», vol. II, p. 408; o logicista: cfr. la reinterpretazione di tali assiomi, riportata *ibid.*, ma soprattutto l'articolo «Logica» in questa *Enciclopedia*, vol. VIII, in particolare pp. 519-20) per poter asserire di *conoscere i numeri*: occorre, per Hilbert come per Bourbaki, cimentarsi con quelle «sfide all'umano ingegno» che i problemi «particolari» rappresentano [cfr. per tutti Dieudonné 1977, p. XII]. Per questo in Hilbert [1900] emergono come stimoli di progresso matematico non pochi problemi di quella che viene detta comunemente, anche se con una certa improprietà, *teoria* dei numeri: «Irrazionalità e trascendenza di certi numeri» (problema VII), «problemi concernenti i numeri primi» (problema VIII), «dimostrazione della legge di reciprocità piú generale in un corpo qualsiasi di numeri» (problema IX), «possibilità di soluzione di una equazione di Diofanto» (problema X), «forme quadratiche a coefficienti algebrici qualsiasi» (problema XI), «estensione del teorema di Kronecker sui corpi abeliani a un dominio di razionalità algebrico qualsiasi» (problema XII).

Non è scopo del presente articolo delineare, seppure schematicamente, la mappa delle regioni della matematica che le ricerche relative a tali problemi hanno delineato facendo emergere connessioni impreviste [il lettore è rimandato ai relativi articoli in Browder 1976], dato che non è la teoria dei numeri l'argomento specifico dell'articolo stesso, bensí quella «famiglia di concetti» che ha preso vita (per rimanere nella tradizione dell'Occidente e per non risalire piú oltre!) da uno «strano» antenato, l'ἀριθμός greco, talora articolando il paradigma originario, talora, invece, movendo controcorrente. In questo paragrafo si esemplificherà – con una scelta inevitabilmente soggettiva – con uno dei problemi aritmetici di Hilbert [1900] per dare almeno un'idea di questa crescita *dei* problemi e *attraverso* i problemi. La scoperta dei «ponti» è, tra l'altro, il problema della stessa *Enciclopedia*: l'immersione nello specifico dei singoli articoli come premessa per la scoperta di interconnessioni nel piano globale dell'*Enciclopedia* stessa.

4.2. La distribuzione dei primi.

«Da tempo immemorabile gli indiani sono eccellenti matematici e hanno in questo campo delle capacità del tutto peculiari. Ho sentito a proposito di un loro scienziato il seguente aneddoto: un amico europeo gli chiese una volta per scherzo se 1729, il numero di matricola del taxi di cui egli si era appena servito, fosse un numero nefasto; con tutta naturalezza egli replicò: "Niente affatto, al contrario 1729 è un numero molto interessante. È il primo numero che può essere espresso in due maniere differenti come somma di due cubi, dal momento che 10^3+9^3 e 12^3+1^3 fanno entrambi 1729"» [Péter 1957, trad. it. p. 68]. Insomma, per gli Indiani, almeno per lo scienziato dell'aneddoto, i numeri anche di quattro cifre sono una sorta di «amici personali»: al contrario, nella nostra scuola, si attribuisce un simile «carattere individuale» [*ibid.*] solo a numeri molto piccoli. Si «colora», per cosí dire, la successione dei numeri fino a 10 o poco piú oltre; gli Indiani, invece, non arretrano di fronte a grandi numeri di quattro cifre (o qualche cifra in piú). Ma ciò è ancora niente davanti alla successione infinita degli stessi naturali 1, 2, 3, ..., 1729, ... Solo un demone come quello di Laplace o l'eroe di qualche racconto di Borges può «colorare» l'intera successione dei numeri... A noi, come alle nostre macchine, anche le piú raffinate, non resta, da un certo punto in poi, che smettere di contare e chiudere con l'indeterminato «molti» la successione dei numeri.

Ma il disporre di una successione infinita come «oggetto» matematico permette, in un senso un po' sofisticato, di superare questa ovvia *impasse* psicolo-

gica. Ciò comporta nuovi problemi, e mette in evidenza la natura «meravigliosa» (nel senso che attribuivano i Greci alla parola) dei numeri. Molti celebri problemi di aritmetica sono nati da elementari considerazioni sulle quattro operazioni in **N**. Per esempio, in **N** è immediato constatare che *ogni* numero è divisibile per se stesso e per l'unità (*uno* è ancora una volta «eccezionale»: per l'unità questi due divisori banali coincidono!) Ma ci sono numeri, come 4, 6, 8, ecc., che ammettono come divisori anche numeri diversi da se stessi e dall'unità; altri numeri come 2, 3, 5, ecc. non godono invece di questa proprietà. Sono i cosiddetti numeri «primi». Essi, in un qualche modo, consentono di «strutturare» la successione dei naturali, un po' come i mattoni forniscono la struttura di un edificio.

Da Euclide a Eulero. La prima rappresentazione sistematica dei naturali e delle loro proprietà di divisibilità si trova negli *Elementi*. Qui Euclide presenta un algoritmo per trovare il massimo comun divisore di due numeri naturali (un algoritmo per molti versi diventato paradigmatico; si veda, in questa stessa *Enciclopedia*, l'articolo «Algoritmo», vol. I, in particolare le pp. 280-301); dimostra inoltre che se p è un numero primo che divide il prodotto ab, allora esso divide a o b. Euclide prova addirittura che esiste un'infinità di numeri primi (cfr. l'articolo «Divisibilità», vol. V, p. 17). Ma «può sembrare strano che, spintosi cosí lontano, Euclide non dimostri il "teorema fondamentale dell'aritmetica", cioè che ogni numero naturale può scriversi come prodotto di numeri primi e che questa rappresentazione è unica a meno dell'ordine dei fattori. La ragione di questa omissione è semplice: Euclide non disponeva di alcun calcolo formale per la moltiplicazione e per l'elevazione a potenza. Era semplicemente impossibile per lui enunciare il teorema e *a fortiori* dimostrarlo» [Ellison 1978, pp. 269-70]. La prima dimostrazione pubblicata di questa verità già risaputa nella tradizione matematica si trova nelle *Disquisitiones Arithmeticae* di Gauss [1801].

C'è come una sorta di lacuna: dopo Euclide occorre attendere fino a Eulero che nel 1737 dà una nuova dimostrazione dell'infinità dei numeri primi. La dimostrazione euleriana lega strettamente l'«aritmetica» intesa come studio delle quantità discrete all'«analisi», studio di quantità continue. Si procede per assurdo. Sia $p_1, p_2, \ldots, p_N$ un elenco completo di tutti i numeri primi. Per $s>1$, Eulero considera il prodotto

$$(1)\qquad \prod_{i=1}^{N}\left(1-\frac{1}{p_i^s}\right)^{-1}=\prod_{i=1}^{N}\left(1+\frac{1}{p_i^s}+\frac{1}{p_i^{2s}}+\ldots\right).$$

Ogni prodotto di numeri primi appare esattamente una volta nel secondo membro di (1) e in forza del «teorema fondamentale dell'aritmetica» (che Eulero conosce ma non dimostra in modo esplicito) ogni frazione $1/n^s$, $s>1$ appare esattamente una volta nello sviluppo in parentesi al secondo membro di (1), sicché Eulero ha

$$(2)\qquad \prod_{i=1}^{N}\left(1-\frac{1}{p_i^s}\right)^{-1}=\sum_{n=1}^{\infty}\frac{1}{n^s}.$$

Per $s=1$ il primo membro della (1) è finito, mentre il secondo membro è una serie divergente: dunque, una contraddizione.

Nella dimostrazione di cui sopra i punti essenziali sono da una parte il legame che emerge fra il «teorema fondamentale dell'aritmetica» e l'infinità dei numeri primi, e dall'altra l'impiego di un teorema tipicamente analitico, cioè la divergenza della serie armonica che figura al secondo membro della (2) nella dimostrazione di un teorema aritmetico. (Eulero, tra l'altro, si spinge oltre la semplice dimostrazione dell'infinità dei numeri primi, in quanto dimostra pure che la «somma» $\Sigma(1/p)$ presa su tutti i primi è divergente).

È sintomatico che, piú tardi, lo stesso Eulero, commentando la ridda di ipotesi circa la distribuzione dei primi entro la successione dei naturali abbia scritto: «I matematici hanno tentato fino ad ora, vanamente, di scoprire qualche ordine nella progressione dei numeri primi e pare lecito credere che si tratti di un mistero che lo spirito umano non saprà mai penetrare. Per convincersene è sufficiente gettare uno sguardo sulla tavola dei primi che certuni si son dati la pena di continuare oltre centomila e ci si accorgerà subito che non vi regna alcuno ordine o regola» [1751, ed. 1911-57 II, p. 241].

Legendre, Gauss e il «teorema» dei numeri primi. Eulero pone cosí i propri risultati come una sorta di colonne d'Ercole: *non oltre!* Ma nell'evoluzione delle matematiche non è nuovo il caso di chi riesce ad attraversare tali colonne, solcando quindi con successo «l'immenso oceano» (il termine è di Cavalieri, a proposito degli indivisibili: ma è metafora ricorrente nella storia del pensiero matematico) che gli si apre davanti. Come nella modellizzazione di molti processi reali un'operazione di media (una sorta di «socchiudere gli occhi») permette di trascurare i dettagli troppo fini di una morfologia per conservarne un'apparenza media che reintroduce la regolarità [cfr. Thom 1971, p. 3], cosí, fin dal 1785, per esempio, Legendre tralascia la spiegazione della struttura «profonda» dei numeri primi per chiedersi invece se ci sia una certa *regolarità* nel comportamento *medio* dei primi. Posta cosí la questione, la risposta di Legendre consiste nel dire che $\pi(x)$, cioè il numero dei primi minori di x, è «approssimativamente» uguale ad $Ax/(B\log x+C)$, ove A, B, C sono certe costanti numeriche. Si tratta di una sorta di congettura pressoché empirica, in quanto estrapolata da tavole di numeri primi minori di 40 000. Successivamente, grazie a ulteriori «osservazioni» numeriche, Legendre migliora la sua formula nella

$$(3)\qquad \pi(x)\sim\frac{x}{\log x-1{,}08366}.$$

Un approccio per molti versi simile è quello di Gauss. Questi muove dall'idea di contare i primi per «blocchi» di un migliaio di naturali consecutivi. Una buona approssimazione della densità media dei primi nell'intorno di un numero abbastanza «grande» x è $1/\log x$. Dunque come approssimazione di $\pi(x)$ Gauss fornisce

$$(4)\qquad \pi(x)\sim\int_2^x\frac{du}{\log u}$$

ove l'integrale al secondo membro è il cosiddetto «logaritmo integrale», notato usualmente $\mathrm{li}(x)$ (cfr. anche «Divisibilità», vol. V, in particolare p. 18). Ora, apparentemente i due risultati (3) e (4), rispettivamente di Legendre e di Gauss, sono differenti, ma, grazie a un'integrazione per parti

$$\int_2^x \frac{du}{\log u} = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{du}{(\log u)^2} = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right)$$

risultano *asintoticamente* equivalenti (per la notazione di Landau $O(g(x))$ cfr. «Calcolo», vol. II, p. 422). È una notevole applicazione dell'ottica *maggiorare/minorare/approssimare* che si viene articolando nel calcolo (cfr. ancora *ibid.*, in particolare pp. 421-23).

«Non sappiamo veramente come Legendre e Gauss abbiano interpretato le loro approssimazioni di $\pi(x)$ a partire dalle loro tavole numeriche. L'uno e l'altro hanno calcolato la differenza tra $\pi(x)$ e la loro formula, ma solo perché pensavano che tale differenza fosse limitata. Tuttavia Gauss ha congetturato che si avesse sempre $\pi(x) < \mathrm{li}(x)$ (ma questa congettura è falsa...) In ultima analisi, si può concludere che entrambi abbiano pensato che le loro formule fossero asintoticamente equivalenti a $\pi(x)$» [Ellison 1978, p. 272], cioè

$$\lim_{x\to\infty} \frac{\pi(x)}{x}(\log x - 1{,}08633) = 1 \qquad \lim_{x\to\infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1$$

da cui segue la piú semplice asserzione

$$(5) \qquad \lim_{x\to\infty} \pi(x)\frac{\log x}{x} = 1$$

divenuta quindi celebre come «teorema dei numeri primi».

La svolta riemanniana. Il «teorema dei numeri primi» è, fino a questo punto, una semplice congettura, una sorta di asserto, si potrebbe dire con una terminologia già introdotta in questa *Enciclopedia* (si veda per esempio l'articolo «Matematiche»), «quasi empirico». Come si trasformi in un teorema nel senso usuale del termine, è istruttivo per piú versi. Nel 1848 Čebyšev mostra che *se* il limite del primo membro della (5) esiste, *allora* il suo valore è 1. Due anni dopo ottiene

$$(6) \qquad 0{,}92129 \le \liminf_{x\to\infty} \pi(x)\frac{\log x}{x} \le 1 \le \limsup_{x\to\infty} \pi(x)\frac{\log x}{x} \le 1{,}105548$$

successivamente perfezionato da Sylvester. Ma ben presto ci si rende conto che i ragionamenti combinatori utilizzati non riescono ancora a dimostrare *l'esistenza* del limite.

Ma il punto che qui vale la pena enfatizzare è che Čebyšev, come già Eulero (cfr. la (2)), prende in considerazione la relazione:

$$(7) \qquad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{i=1}^{\infty}\left(1 - \frac{1}{p_i^s}\right)^{-1}$$

ove s è una variabile *reale*. Ma se è ormai chiaramente emerso che vi è una stretta relazione tra la funzione $\zeta(s)$ e i numeri primi, lo slittamento fondamentale del problema avviene con Riemann [1859], «probabilmente l'articolo piú importante pubblicato sui numeri primi» [Ellison 1978, p. 275]: la chiave della comprensione profonda di tale relazione si rivela qui la considerazione della funzione $\zeta(s)$ come una funzione della variabile *complessa* s. (È lo stesso Riemann che mostra come $\zeta(s)$ possa venir prolungata analiticamente nel piano complesso).

È sostanzialmente certo che Riemann mirasse a dimostrare il teorema dei numeri primi: ora, anche se egli non raggiunge lo scopo, offre un certo numero di congetture destinate a fornire la nervatura della ricerca successiva. (Tali congetture sono riportate qui seguendo le notazioni ormai usuali; in particolare, per ogni numero complesso $s = a + ib$, si scriverà $\mathrm{Re}(s)$, $\mathrm{Im}(s)$ per a e b rispettivamente):

a) $\zeta(s)$ ha un'infinità di zeri complessi (cioè di numeri complessi s tali che $\zeta(s) = 0$), simmetrici rispetto alle rette $\mathrm{Re}(s) = 1/2$ e $\mathrm{Im}(s) = 0$.

b) La funzione $\xi(s) = (1/2)s(s-1)\pi^{-(1/2)s}\Gamma(s/2)\zeta(s)$, ove Γ è la cosiddetta funzione gamma di Eulero, si può scrivere nella forma

$$\xi(s) = e^{A+Bs}\prod_{\rho}\left(1 - \frac{s}{\rho}\right)e^{s/\rho}$$

ove A, B sono costanti e il prodotto è preso per ρ che percorre tutti gli zeri complessi di $\zeta(s)$.

c) Se $N(T)$ designa il numero degli zeri di $\zeta(s)$ nel rettangolo $0 \le \mathrm{Re}(s) \le 1$, $|\mathrm{Im}(s)| \le T$, allora

$$N(T) = \frac{T}{2\pi}\log\left(\frac{T}{2\pi}\right) - \frac{T}{2\pi} + O(\log T).$$

d) Tutti gli zeri complessi di $\zeta(s)$ si trovano su $\mathrm{Re}(s) = 1/2$.

e) Per $x > 1$ si può definire una funzione $\Pi(x)$ ponendo $\Pi(x) = \sum_{p^m \le x} \frac{1}{m}$.

Questa funzione è legata alla funzione $\pi(x)$ in quanto

$$\Pi(x) = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \ldots = \pi(x) + O(\sqrt{x}).$$

Riemann congettura allora che, per x non intero, si abbia la formula esplicita

$$(8) \qquad \Pi(x) = \mathrm{li}(x) - \sum_{\rho}\mathrm{li}(x^{\rho}) + \int_0^{\infty}\frac{du}{(u^2-1)\,u\log u} - \log 2$$

ove la somma va estesa a tutti gli zeri complessi di $\zeta(s)$. È proprio la (8) che esplicita la relazione tra gli zeri di $\zeta(s)$ e il valore di $\pi(x)$.

a) e *b*) sono state dimostrate per la prima volta da Hadamard nel 1893 e hanno a loro volta svolto un ruolo importante nelle prime dimostrazioni del teorema dei numeri primi. L'asserzione *c*) è stata dimostrata da Mangoldt nel 1895 con un lieve errore, poi corretto nel 1905. Sempre a Mangoldt si deve la

dimostrazione della formula esplicita *e*). Sulla asserzione *d*) si tornerà in seguito (pp. 931-33).

L'approccio di Dirichlet. Esso precede, cronologicamente, la svolta segnata da Riemann [1859], e rappresenta un'articolazione del punto di vista di Eulero (cfr. in particolare la (2)) inaugurando – dopo il carattere relativamente casuale dei lavori di un Jacobi e dello stesso Eulero – una fase sistematica di applicazione delle funzioni analitiche nella teoria dei numeri [cfr. per tale valutazione Kline 1972, p. 829].

Nel 1785 Legendre aveva congetturato che se a e q sono primi tra loro, la progressione aritmetica $nq+a$, $n=1, 2, \ldots$ contiene una infinità di primi. È una generalizzazione dell'ordine di idee espresso dal teorema di Euclide, ma di cui manca, fino a Dirichlet, una dimostrazione generale. Il punto di partenza dell'approccio di Dirichlet è ancora Eulero, in particolare la sua dimostrazione della divergenza della serie Σp^{-1} (cfr. p. 925). Lo scopo di Dirichlet è di stabilire che, per a e q primi tra loro, la serie resta divergente limitandosi ai numeri primi tali che $p \equiv a \pmod q$ (per la nozione di congruenza, cfr. l'articolo «Calcolo» in questa stessa *Enciclopedia*, vol. II, p. 394).

La novità sta innanzitutto nell'utilizzazione dei cosiddetti *caratteri* modulo q (per q intero positivo qualsiasi, $\chi(n)$ è una funzione aritmetica a valori complessi, periodica di periodo q, nulla sugli n che non sono primi con q e soddisfacenti le relazioni $\chi(1)=1$, $\chi(mn)=\chi(m)\chi(n)$) per generalizzare l'identità di Eulero nella

$$(9) \qquad L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}=\prod_p(1-\chi(p)p^{-s})^{-1}$$

ove $s>1$: Dirichlet resta però al di qua, per cosí dire, della svolta riemanniana (cfr. p. 927), in quanto la generalizzazione dell'identità di Eulero (2) non concerne valori complessi, ma solo reali della variabile s.

Dalla (9) Dirichlet ottiene, passando ai logaritmi:

$$(10) \qquad \log L(s,\chi)=-\sum_p \log\left(1-\frac{\chi(p)}{p^s}\right)=\sum_p\sum_{m=1}^{\infty}\frac{\chi(p^m)}{mp^{ms}}.$$

Per isolare, al secondo membro della (10), la somma Σp^s per $p\equiv a \pmod q$ Dirichlet moltiplica la (10) per $\bar\chi(a)$ (ove $\bar\chi(a)$ designa il complesso coniugato di $\chi(a)$) e somma su tutti i caratteri, sicché:

$$\sum_\chi \bar\chi(a)\,L(s,\chi)=\sum_\chi\sum_p\sum_{m=1}^{\infty}\frac{\bar\chi(a)\chi(p^m)}{mp^{ms}}.$$

A questo punto emerge l'importanza dei caratteri di Dirichlet, in quanto essi sono costruiti in modo da verificare le relazioni

$$(11) \qquad \frac{1}{\varphi(q)}\sum_\chi \bar\chi(a)\chi(n)=\begin{cases}1 & \text{se } n\equiv a \pmod q\\ 0 & \text{altrimenti}\end{cases}$$

ove $\varphi(q)$ denota il numero delle classi residue modulo q. Applicando la (11) si ottiene

$$(12) \qquad \frac{1}{\varphi(q)}\sum_\chi \bar\chi(a)\log L(s,\chi)=\sum_{\substack{p\equiv a\\ (\mathrm{mod}\, q)}} p^{-s}+\sum_{m=1}^{\infty}\sum_{\substack{p^m\equiv a\\ (\mathrm{mod}\, q)}}\frac{p^{-ms}}{m}.$$

In (12) si mostra facilmente che la doppia somma al secondo membro è convergente per $s\geq 1$. Il «teorema» di Legendre sarà allora dimostrato una volta che si sia provato che $\sum_\chi \bar\chi(a)\log L(s,\chi)$ tende all'infinito per s tendente a 1. Ora, la funzione $L(s,\chi)$ ove χ_0 è il cosiddetto carattere principale (cioè il carattere χ tale che $\chi(n)=1$ se n e q sono primi tra loro) è un multiplo della funzione $\zeta(s)$ di cui a p. 927 e tende all'infinito per s tendente a 1. Cosí $\lim_{s\to 1}\chi_0(a)\log L(s,\chi_0)=+\infty$.

Resta infine da dimostrare che, per $\chi\neq\chi_0$ ogni termine $\log L(s,\chi_0)$ della (12) è limitato per s tendente a 1. Dirichlet riesce a mostrare che, se $\chi\neq\chi_0$, $L(s,\chi)$ converge per $s>0$ e rappresenta una funzione continua (è un'applicazione del celebre «criterio di Dirichlet» per le serie infinite). Di conseguenza il fatto che $\log L(s,\chi)$ sia limitato per s tendente a 1 equivale a $L(1,\chi)\neq 0$: la verifica di quest'ultimo passo è la pietra terminale della dimostrazione (tale verifica è ottenuta da Dirichlet nel corso della dimostrazione, *via* le funzioni $L(s,\chi)$, di una celebre formula che dà il numero delle classi di forme quadratiche binarie di dato discriminante; cfr. p. 939).

Il teorema dei numeri primi. Dimostrazioni analitiche e dimostrazioni «elementari». Come nel caso del teorema di Eulero (p. 925), si ha nel procedimento di Dirichlet un teorema di aritmetica come conseguenza di un risultato analitico. Lo stesso può dirsi per l'ordine di idee che porta a stabilire la congettura riemanniana *e*) di p. 927. E, in un certo senso, i due approcci – quello di Dirichlet e quello di Riemann –, che si biforcano da un medesimo archetipo (la formula (2) di Eulero), trovano una prima ricomposizione nelle ricerche che si incentrano intorno alla dimostrazione del teorema dei numeri primi, dovuta nel 1896, indipendentemente, a Hadamard e a La Vallée-Poussin. Tre anni dopo La Vallée-Poussin pubblica uno studio dettagliato dell'approssimazione di $\pi(x)$ mediante le due funzioni $\mathrm{li}(x)$ e $x/\log x$, in cui mostra che $\mathrm{li}(x)$ è la miglior approssimazione e che, di fatto,

$$(13) \qquad \pi(x)-\mathrm{li}(x)=O(x\exp(-c\sqrt{\log x}))$$

ove c è una costante positiva che La Valleé-Poussin riesce a determinare esplicitamente.

Una volta dimostrato il teorema dei numeri primi, è relativamente facile stabilirne l'analogo per i primi in una progressione aritmetica (cfr. p. 928). Il fatto che la teoria delle funzioni di variabile complessa sviluppata per la funzione zeta di Riemann si applichi anche alle funzioni L di Dirichlet, permette di *tradurre*, per cosí dire, le asserzioni riemanniane relative a $\zeta(s)$ in asserzioni analo-

ghe per $L(s,\chi)$ e le dimostrazioni sono degli adattamenti molto naturali delle dimostrazioni di cui si dispone per $\zeta(s)$.

Non c'è quindi da stupirsi che nello stesso 1896 Hadamard e La Vallée-Poussin abbiano dimostrato per $\pi(x,q,a)$, cioè per la funzione che dà il numero dei primi minori di x nella progressione $\{nq+a\}$ di p. 928, la formula asintotica

$$(14) \qquad \lim_{x\to\infty} \pi(x,q,a)\cdot\frac{\log x}{x}=\frac{1}{\varphi(q)}$$

a suo tempo congetturata da Legendre e che, nel 1899, La Vallée-Poussin abbia esteso a $\pi(x,q,a)$ la stima (13).

Occorrono qui tre ulteriori considerazioni:

1) Il Novecento vede un miglioramento della stima di $\pi(x)-\mathrm{li}(x)$. Nel 1921 Littlewood, sviluppando un'idea di Weyl, ottiene con un brillante metodo delle correzioni non banali nella (13): ed è tale metodo, in seguito semplificato da Landau, che è stato ampiamente sviluppato dal sovietico Vinogradov. Il miglior risultato conosciuto è quello di Vinogradov e Korobev (1958):

$$(15) \qquad \pi(x)-\mathrm{li}(x)=O\left\{x\exp\left(-\frac{c(\log x)^{3/5}}{(\log\log x)^{1/5}}\right)\right\}.$$

Si resta però ben lontani dalle stime ottenute supponendo vera la congettura *d*) di Riemann. Ma su questo punto si tornerà fra poco.

2) Il teorema dei numeri primi, i risultati ausiliari come la (13) e le ulteriori correzioni sono ottenute con tecniche di teoria delle funzioni di variabile complessa estremamente complicate. Ben presto è emersa una tendenza alla semplificazione (per esempio, metodo di Landau nella dimostrazione del teorema dei numeri primi, rivelatosi quindi di notevole utilità in teoria «analitica» dei numeri, ecc.), spesso combinata con un'insoddisfazione per il fatto che un enunciato aritmetico in cui compare in modo abbastanza naturale una variabile reale x ricorra per la dimostrazione all'analisi complessa. Ciò ha spinto alla ricerca di dimostrazioni «elementari», che non utilizzino cioè la teoria delle funzioni di variabile complessa, ma solo qualche elemento di analisi reale.

Verso la fine degli anni '20 queste ricerche hanno permesso di accertare che la sola proprietà di $\zeta(s)$ che interviene nella dimostrazione del teorema dei numeri primi è che $\zeta(s)$ non si annulla sulla retta $\mathrm{Re}(s)=1$; si era anche dimostrato che questo fatto, a sua volta, era una semplice conseguenza del teorema dei numeri primi. «Si ha cosí una sorta di equivalenza tra una proprietà analitica di $\zeta(s)$ e il teorema dei numeri primi, che è un puro enunciato della teoria delle funzioni di variabile reale. Ciò ha persuaso i matematici dell'impossibilità di eliminare il ricorso alla teoria di una variabile complessa dalla dimostrazione del teorema dei numeri primi. Ma, come molte idee puramente euristiche, anche questa convinzione è falsa: nel 1948 Erdös e Selberg hanno pubblicato indipendentemente versioni della "dimostrazione elementare" cosí a lungo attesa. Benché di interesse metodologico considerevole, le diverse illustrazioni elementari del teorema dei numeri primi oggi note non hanno però aggiunto molto alla nostra conoscenza della distribuzione dei numeri primi e le correzioni che apportano non sono abbastanza buone quanto quelle ottenute per via analitica» [Ellison 1978, p. 280].

3) Il folclore matematico riporta la leggenda secondo cui a coloro che avessero dimostrato il teorema dei numeri primi sarebbe toccato in premio l'immortalità (Hadamard e La Vallée-Poussin raggiunsero, peraltro, entrambi quasi il secolo). Al fascino della sfida intellettuale si è, evidentemente, sovrapposto anche il significato profondo che comporta questa immersione della successione dei numeri naturali nel continuo dei reali. «Il fatto che vi sia un teorema dei numeri primi significa che, benché i numeri primi siano distribuiti in modo irregolare lungo le sezioni della successione dei numeri che possono venir prese in esame, sono nondimeno soggetti a un qualche tipo di ordine se sono considerati nella loro infinita totalità. Mi viene in mente un paragone che ho letto da qualche parte a proposito del problema del libero arbitrio: se osserviamo da vicino uno sciame di api, ci sembrerà che volino di qua e di là in tutte le direzioni; tuttavia l'intero sciame si muove in una certa direzione verso una meta precisa» [Péter 1957, trad. it. p. 77].

4.3. Un problema aperto: l'ipotesi di Riemann.

«I lavori di teoria analitica dei numeri in genere si limitano a presentare quel che l'autore è in grado di dimostrare, mentre di rado vengono menzionati obiettivi piú ambiziosi. In questa occasione facciamo il contrario elencando le principali congetture e problemi che motivano grandissima parte della teoria analitica dei numeri. Abbiamo bisogno di menzionare solo poche questioni: basterebbero le risposte a queste a fornire la soluzione a un ampio numero di problemi ormai familiari. Si potrebbe obiettare che una lista del genere non è utile, in quanto non fornisce in realtà problemi accessibili, ma penso che giovi avere un'idea piú ampia di quella che è la verità che sospettiamo, rispetto alla quale controllare le nostre idee» [Montgomery 1976, p. 307]. Questo approccio quasi empirico alle questioni aperte è del resto motivato dalla situazione intricata che intorno all'apparentemente «immediata» idea di numero si è venuta formando. Sia lecito qui impiegare una metafora coniata per altra situazione matematica [Bauer 1974, p. 41]: poteva sembrare un tempo che un certo ordine di problemi – come quelli di teoria moltiplicativa dei numeri che si sono fin qui esaminati – costituissero un grande incrocio stradale per molti settori della matematica. «Ora il traffico è cresciuto, gli incroci sono diventati degli snodi di vie sopraelevate» [*ibid.*]: la rilevanza di un problema rispetto a un altro slitta nel tempo e la ricerca stessa può venir modellata con un'immagine piú articolata di quella che la riferisce a un problema «centrale». (Ancora una volta è, metaforicamente, lo stesso problema per l'*Enciclopedia*...)

La storia dell'«ipotesi di Riemann», cioè della congettura *d*) riportata a p. 927, è al proposito significativa. Proprio sull'onda dei successi di Mangoldt, Hadamard e La Vallée-Poussin, Hilbert [1900, ed. 1976 p. 16] si augurava che potesse venir presto decisa anche tale ipotesi. La si riesamini piú nei partico-

lari: la zeta di Riemann (cfr. la (7) di p. 926) $\zeta(s)$ non ha zeri in $\mathrm{Re}\, s \geq 1$ e i soli zeri che ha in $\mathrm{Re}\, s \leq 0$ sono i semplici zeri $s = -2, -4, \ldots, -2n, \ldots$ (zeri banali). Ma nella fascia critica $0 < \mathrm{Re}\, s < 1$ la funzione zeta ha invece una infinità di zeri (detti non banali). La congettura di Riemann consiste nel supporre che tutti gli zeri (non banali) giacciono sulla retta critica $\mathrm{Re}\, s = 1/2$.

Seguendo l'impostazione di Richards si possono distinguere almeno tre linee di attacco all'ipotesi di Riemann. Innanzitutto quella prettamente calcolistica: essa – consistente in un vero e proprio controllo della congettura eseguendo i conti per uno zero dopo l'altro – è una prospettiva di ricerca praticamente perseguibile solo con l'impiego di calcolatori sempre piú rapidi. Ma naturalmente questo tipo di controllo – eseguito finora su piú di tre milioni di zeri – «nulla di definito dice sugli infiniti zeri che restano» [Richards 1978, p. 54]: questo tipo di controllo può solo falsificare l'ipotesi di Riemann. Il fatto che non vi sia riuscito dice solo che la congettura è stata corroborata per i primi tre milioni di zeri e «poco piú». Ma a questo impiego del calcolatore come equivalente del controllo «empirico» della congettura si può affiancare «anche un approccio piú teorico» [*ibid.*] consistente nel determinare con metodi che ovviamente non usino la congettura o un suo equivalente la percentuale degli zeri della $\zeta(s)$ che giacciono sulla retta $\mathrm{Re}\, s = 1/2$. Dopo alcuni classici risultati di Selberg negli anni '40, l'informazione maggiore proviene dalle ricerche di Levinson (1974), il quale ha dimostrato che, degli zeri non banali, *almeno un terzo* si trova sulla retta critica. Resta, infine, l'approccio «creativo»: l'attacco sia diretto sia indiretto dei vari ricercatori al problema, cercando cioè di ottenere la dimostrazione come risultato collaterale di ricerche primariamente intese ad altro obiettivo. È in questa prospettiva che assumono un importante valore ausiliario la gamma di equivalenti e quella di conseguenze dell'ipotesi, su cui già a suo tempo Hilbert [1900] richiamava l'attenzione.

Si tocca qui uno dei nodi piú delicati della ricerca attuale: come del resto mostra in piú punti il presente articolo, la funzione zeta può venir generalizzata in molti modi (funzioni L di Dirichlet, funzione zeta di Dedekind, ecc.), dando origine ad uno studio delle «funzioni zeta» perseguito coi metodi tipici della teoria delle funzioni analitiche. Per tali funzioni, in generale, è possibile allora formulare gli analoghi della congettura riemanniana: si tratta delle cosiddette ipotesi di Riemann *generalizzate*. Anche qui è rilevante il confronto tra quel che tali ipotesi implicano in aritmetica moltiplicativa e altrove e i risultati ottenuti in modo indipendente. Si riconsideri, per esempio, il problema che aveva motivato l'approccio di Dirichlet (cfr. § 4.2, p. 928 in particolare): un importante teorema di Siegel (1936) circa il non annullarsi delle funzioni L di Dirichlet vicino al punto $s = 1$ (una volta che anche esse siano state prolungate analiticamente a tutto il piano della variabile complessa s) permette una stima dell'errore $E(x,q,a) = \pi(x,q,a) - \mathrm{li}(x)/\varphi(q)$ nel teorema dei numeri primi per le progressioni (cfr. anche p. 930): si ricava infatti, per ogni m e n, $E(x,q,a) = O(x/\log^n x)$ uniformemente per $q \leq \log^m x$ con lo svantaggio che la costante (dipendente da m e n) implicita nel simbolo O non è effettivamente calcolabile. La corrispondente ipotesi di Riemann generalizzata implica invece $E(x,q,a) = O(\sqrt{x}\log x)$ uniformemente per $q \leq x$. Ora, in molte applicazioni, questa stima *puntuale* può venir sostituita da un'opportuna *stima di media*, ancora una volta, dunque, «socchiudendo gli occhi» (cfr. p. 925). È questo il significato [cfr. per esempio Chandrasekharan 1974, pp. 3 sgg.] di un profondo risultato dimostrato da Bombieri (1965), sostitutivo per certi versi dell'ipotesi generalizzata:

$$(16) \qquad \sum_{q \leq Q} \max_{y \leq x} \max_{a,(a,q)=1} |E(y,q,a)| \ll x(\log x)^{-A}$$

ove $(a,q) = 1$ abbrevia, al solito, che a e q sono primi tra loro, A è una costante qualsiasi > 0 e Q è definito dalla $Q = x^{1/2}(\log x)^{-B}$ ove $B = B(A)$ è una costante > 0 che dipende da A.

5. *Aspetti della teoria «classica» dei numeri algebrici.*

5.1. Che cos'è un intero (algebrico)?

Esemplari, sia sotto il profilo dell'estensione della nozione di numero sia sotto quello dell'approfondimento delle proprietà piú tipicamente «aritmetiche», sono alcune vicende connesse con la nozione di numero algebrico. Un numero, notoriamente, si dice algebrico (sul corpo **Q** dei razionali) quando è radice di un polinomio in una indeterminata a coefficienti in **Q** (o, il che è lo stesso, di un polinomio a coefficienti in **Z**). Com'è noto – e come è del resto ampiamente trattato in altri articoli di questa stessa *Enciclopedia* – i numeri algebrici, pur includendo come parte propria i razionali, non esauriscono la totalità dei complessi: anzi, ne costituiscono un'esigua minoranza, dato che l'insieme degli algebrici ha solo la potenza del numerabile. Ma, in questa sede, interessa una vera e propria «teoria» dei numeri algebrici, relativamente autonoma dalla dicotomia algebrico/trascendente e piú tarda della semplice comparsa di numeri algebrici nel corso della soluzione di equazioni algebriche di grado non elevato.

L'idea base è quella della costruzione dell'anello di polinomi $\mathbf{Z}[\vartheta]$ a coefficiente in **Z** per ϑ algebrico: già essa appare nella costruzione gaussiana dei cosiddetti «interi di Gauss» (impiegati da questi nel 1831 per lo studio della reciprocità quadratica ove è $\vartheta = i$ unità immaginaria) e, piú oltre, nel contesto delle ricerche di Eisenstein (1844), sulla reciprocità cubica, ove $\vartheta = \rho$ e $\rho^3 = 1$. Ora, «è probabilmente a causa del "buon" comportamento di tali anelli che nessuno, per lungo tempo, sembra essersi accorto che esistono numeri algebrici ϑ per cui l'aritmetica dell'anello $\mathbf{Z}[\vartheta]$ differisce radicalmente dall'aritmetica dei razionali» [Ellison 1978, pp. 191-92]. L'idea che l'aritmetica di $\mathbf{Z}[\vartheta]$ rispecchi quella di **Q** può essere, in realtà, responsabile di curiosi abbagli, su alcuni dei quali si fondano ancora certe ottocentesche «dimostrazioni» della congettura di Fermat [per un esempio cfr. *ibid.*].

Tale congettura, il cosiddetto «ultimo teorema», lasciato senza dimostrazione, a detta di Fermat stesso, semplicemente perché gli mancava lo spazio per

proseguire sul margine del testo di Diofanto su cui appuntava le sue «annotazioni», non è altro che uno dei tanti problemi di «analisi diofantina»: si tratta, notoriamente, di mostrare che l'equazione $x^n+y^n=z^n$ per $n>2$ non ammette soluzioni intere (non banali). Ora la congettura «non ha grande interesse in sé: una dimostrazione completa la priverebbe dell'aura di magia che la circonda», commentava Dickson [1919-23, ed. 1952 II, p. XIX]. La «dimostrazione completa» non è stata ancora trovata: l'alone di magia è rimasto... Eppure, Dickson ha sostanzialmente ragione quando soggiunge che la congettura «se ha acquistato una posizione di rilievo nella storia della matematica è perché ha fornito l'ispirazione che portò Kummer a inventare i suoi numeri ideali, dai quali si sviluppò la teoria generale dei numeri algebrici che è oggi una delle branche piú significative della matematica» [*ibid.*].

È noto che Kummer riuscí a dimostrare, per una classe estesissima di numeri primi p, che $x^p+y^p=z^p$ non ammette soluzioni intere (non banali). Non riuscí però a dimostrare la congettura per *tutti* i numeri *primi*: «Certi numeri primi eccezionalmente agili sfuggirono alla sua rete e vi sfuggono ancora» [Bell 1937, trad. it. p. 520]. Ma dal 1835 al 1847 Kummer sviluppò le ricerche che dovevano culminare «nell'introduzione dei numeri ideali e nella scoperta del teorema della scomposizione univoca dei numeri di un corpo ciclotomico in fattori primi ideali, teorema che, grazie all'estensione fattane successivamente da Dedekind e da Kronecker ai dominî algebrici qualsiasi, è divenuto il punto centrale della teoria moderna dei numeri e ha oggi un'importanza che va oltre i limiti di questa teoria, fino a spingersi nelle regioni dell'algebra e della teoria delle funzioni» [Hilbert 1900, ed. 1976 p. 2].

Qui si articolerà, in particolare, il punto di vista di Dedekind (1871-93). Una ragione va cercata nel fatto che, pur preceduto da Abel e Galois con la loro idea di «dominio di razionalità», Dedekind è sostanzialmente il primo matematico che definisce formalmente il concetto di *corpo* (per cui si veda l'articolo «Calcolo», vol. II, p. 393) e considera, sistematicamente, sottocorpi del corpo complesso **C**, in particolare *corpi di numeri algebrici* K, di grado n su **Q**, cioè estensioni finite di **Q**.

Ciò premesso, si riconsideri la costruzione dei razionali (con segno) **Q** a partire dall'anello degli interi (relativi) **Z** (cfr. le regole Q.1-Q.3 riportate in «Calcolo», vol. II, p. 412) e, conseguentemente, l'immersione canonica di **Z** in **Q**: lo scopo di gran parte della teoria dei numeri algebrici dell'Ottocento si può allora caratterizzare come la generalizzazione «corretta» [Ellison 1978, p. 291] dell'aritmetica degli interi **Z** in **Q**. Ma qual è in K il «candidato» opportuno per l'analogo di **Z** in **Q**? Un primo tentativo di Dedekind mirante a costruire una fattorizzazione unica per l'anello $\mathbf{Z}[\vartheta]$ con ϑ algebrico era destinata ben presto a fallire. Né miglior fortuna ebbero i tentativi di altri matematici intesi a definire la nozione di «intero algebrico» in modo da avere fattorizzazione unica in interi algebrici «primi».

La domanda «Che cos'è un intero?» (ovviamente nel contesto K) riceve da Dedekind risposta grazie ad un'indagine astratta (assiomatica) delle condizioni che dovrebbe ragionevolmente soddisfare un insieme di numeri algebrici

suscettibili di essere chiamati «interi algebrici». Si tratta di imporre, per ciascun K, che:

a) i soli elementi di **Q** che sono degli «interi algebrici» sono gli elementi di **Z**;
b) la definizione di «intero algebrico» deve essere tale che se L è un'estensione di K, gli interi algebrici di K restano interi algebrici di L;
c) gli interi algebrici formano un anello;
d) se α è un intero algebrico, tutti i coniugati di α sono interi algebrici.

Ed è da queste condizioni che risulta: 1) le funzioni simmetriche (per cui si veda, per esempio, l'articolo «Invariante» in questa stessa *Enciclopedia*, vol. VII, p. 893) di α e dei suoi coniugati devono dare degli interi algebrici; ma, 2) poiché α è algebrico, le funzioni simmetriche di α dànno valori in **Q**. Dunque da 1) e 2) si ottiene che i valori delle funzioni simmetriche di α sono degli interi $a_i \in \mathbf{Z}$. Quindi α è un *intero algebrico* (di K) se e solo se annulla un polinomio monico a coefficienti interi ovvero è soluzione di un'equazione

$$(1) \qquad x^n+a_1x^{n-1}+\ldots+a_n=0 \qquad \text{con } a_i \in \mathbf{Z}.$$

È immediato mostrare che l'insieme degli interi algebrici di K cosí definiti forma un sottoanello di K e il corpo delle frazioni di tale sottoanello – costruito secondo regole che costituiscono l'analogo formale delle Q.1-Q.3 di «Calcolo» (vol. II, p. 412) – riproduce proprio K. Non è il solo anello incluso in K che riproduce K in questo modo: ma, osserva Dedekind, O_K è quello massimale.

Di piú, si può mostrare che O_K è uno **Z**-modulo libero di rango $n=[K:\mathbf{Q}]$. Data una base $\alpha_1, \ldots, \alpha_n$ si chiama discriminante del corpo K il numero

$$(2) \qquad D(O_K)=\begin{vmatrix} \alpha_1^{(1)} & \ldots & \alpha_1^{(n)} \\ \vdots & & \vdots \\ \alpha_n^{(1)} & \ldots & \alpha_n^{(n)} \end{vmatrix}$$

ove $\alpha_i^{(j)}$ designa lo j-esimo coniugato di α_i. Il numero $D(O_K)$, che verrà abbreviato D_K, è razionale e non dipende dalla scelta di una base particolare di O_K. Sussiste il teorema che per $K \neq \mathbf{Q}$ è $|D_K|>1$ (Minkowski, 1891). Inoltre, per ogni intero m di **Z** c'è solo un numero finito di corpi algebrici K tali che $D_K=m$. Su questo importante risultato (Hermite e Minkowski, 1896) – ottenuto impiegando tecniche della cosiddetta «geometria dei numeri» – si tornerà nel § 6.2.

5.2. Gli ideali.

O_K è anche l'ambito adeguato per la generalizzazione ai numeri algebrici della teoria classica della divisibilità, in quanto, al contrario che nel corpo K, la proposizione α *divide* β (in simboli $\alpha \mid \beta$) resta una particolarità, proprio come lo è, del resto, in **Z**. Ma già nella ricerca di un analogo del «teorema fondamentale dell'aritmetica» (cfr. p. 934) si incontra una serie di difficoltà (per

esempio, in $K = \mathbf{Q}(\sqrt{-5})$, gli interi algebrici non ammettono in generale una fattorizzazione unica (cfr. «Divisibilità», vol. V, p. 30)).

Dedekind ha ristabilito questa unità sfruttando appunto quelli che ha chiamato «ideali». Ora «la nozione di un "ideale" non è difficile ad afferrarsi, benché ci sia un "ma" (*la classe piú inclusiva divide la classe meno inclusiva* come spiegheremo fra poco) che urta il senso comune; ma il senso comune è fatto per essere urtato; se tutte le nostre facoltà fossero immuni da urti, saremmo una razza di cretini. Un "ideale" deve possedere almeno due proprietà; lasciare l'aritmetica ordinaria (razionale) essenzialmente qual è, obbligare gli interi algebrici, piú o meno recalcitranti, a obbedire a questa legge fondamentale dell'aritmetica che essi sfidano; la scomposizione *unica* in numeri primi» [Bell 1937, trad. it. p. 529].

La questione della classe piú inclusiva che divide la classe meno inclusiva è in relazione col fenomeno seguente (e con la sua generalizzazione, come si vedrà). Si sa che 2 divide 4 *aritmeticamente*, cioè senza resto; al posto di questo fatto evidente che non conduce a nulla se lo si applica ai corpi di numeri algebrici, si sostituisca 2 con la *classe di tutti i suoi multipli* interi, ..., −8, −6, −4, −2, 0, 2, 4, 6, 8, ...; per comodità, si rappresenti questa classe con (2); allo stesso modo, (4) rappresenterà la classe di *tutti* i multipli interi di 4; fra questi, alcuni sono ..., −16, −12, −8, −4, 0, 4, 8, 12, 16, ... È evidente che (2) è la classe piú inclusiva; infatti, essa contiene *tutti* i numeri di (4) e inoltre, per non citarne che due, −6 e 6. Si rappresenta il fatto che (2) contiene (4) col simbolo $(2)|(4)$. Si può facilmente vedere che se μ, ν sono numeri interi, si ha $(\mu)|(\nu)$ *quando, e solo quando,* μ *divide* ν.

Questo potrebbe suggerire l'idea di sostituire la nozione di divisibilità aritmetica con quella d'inclusione di classi, ma tale sostituzione sarebbe vana se non conservasse le proprietà caratteristiche della divisibilità aritmetica. Fortunatamente tali proprietà sono conservate. La conclusione è che la sostituzione dei numeri con le loro classi corrispondenti risponde a ciò che si cerca se si aggiunge la definizione di «moltiplicazione». Si definisce ad esempio $(\mu) \times (\nu)$ come la classe $(\mu\nu) : (2) \times (6) = (12)$. Si noti che questa è una definizione, e non significa che essa risulti dai significati di (μ) e (ν).

Gli ideali di numeri algebrici di Dedekind sono le generalizzazioni di ciò che precede. Secondo la sua abitudine, Dedekind ne dà una definizione *astratta*, cioè basata su delle proprietà formali piuttosto che su una relazione con qualche particolare maniera di rappresentare o di descrivere la cosa definita.

Si consideri l'insieme O_K di *tutti* i numeri *interi* algebrici contenuti in un corpo K; in questo insieme ci sono dei sottoinsiemi. Un sottoinsieme α è detto *ideale* se possiede le due proprietà seguenti:

1) la somma e la differenza di due interi qualsiasi di α si trovano in α;
2) se si moltiplica un intero qualsiasi di α con un intero qualsiasi di O_K, l'intero che ne risulta si trova in α.

Un ideale è dunque una classe *infinita* d'interi. Si vede facilmente che (μ), (ν), ..., definiti sopra, sono degli ideali secondo 1), 2). Come si è detto prima, se un ideale ne contiene un altro, si dice che il primo ideale divide il secondo.

Si può dimostrare che ogni ideale è un insieme di numeri interi della forma

$$(3) \qquad \gamma_1\alpha_1 + \gamma_2\alpha_2 + \ldots + \gamma_n\alpha_n$$

dove $\alpha_1, \alpha_2, \ldots, \alpha_n$ sono degli interi *determinati* nel corpo K di grado n in questione, e dove ognuno dei $\gamma_1, \gamma_2, \ldots, \gamma_n$ può essere un intero qualunque del corpo. Ciò dato, è comodo rappresentare un ideale scrivendo i soli interi fissi $\alpha_1, \alpha_2, \ldots, \alpha_n$, e lo si fa prendendo $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ come simbolo dell'ideale.

Bisogna ora definire la moltiplicazione degli «ideali». Il prodotto di due ideali $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $(\beta_1, \beta_2, \ldots, \beta_n)$ è l'ideale il cui simbolo è $(\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_n, \alpha_2\beta_1, \alpha_2\beta_2, \alpha_2\beta_n, \ldots, \alpha_n\beta_n)$, nel quale si trovano tutti i prodotti possibili ottenuti moltiplicando un intero del primo simbolo con un intero del secondo; per esempio, il prodotto di (α_1, α_2) per (β_1, β_2) è $(\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2)$. È sempre possibile ridurre tale simbolo di prodotto, per K di grado n, a un simbolo contenente tutt'al piú n interi.

Un ideale il cui simbolo non contiene che *un* intero, per esempio (α_1), si chiama un ideale *principale*. Impiegando la notazione $(\alpha_1)|(\beta_1)$ per esprimere che (α_1) *contiene* (β_1), si vede senza difficoltà che si può scrivere $(\alpha_1)|(\beta_1)$ *quando, e solo quando,* l'intero α_1 *divide* l'intero β_1. Allora, come sopra, la nozione di divisibilità aritmetica è in questo caso, per interi algebrici, completamente equivalente a quella d'inclusioni di insiemi. Un ideale *primo* è un ideale che non è divisibile per, o incluso in un ideale qualsiasi, salvo l'«ideale» generale O_K, che comprende *tutti* gli interi algebrici nel corpo dato. Se si sostituiscono gli interi algebrici con i loro ideali principali corrispondenti, resta provato che un ideale dato è il prodotto di ideali primi in un'unica maniera, esattamente come nel teorema fondamentale dell'aritmetica un intero razionale è il prodotto di numeri primi in una maniera sola.

5.3. Confronto tra gli ideali di Dedekind e i «numeri ideali» di Kummer.

Sarà infine istruttivo confrontare la nozione dedekindiana di ideale (intero) con la primitiva intuizione di Kummer. Un ideale, nel senso di Dedekind, «non è un numero, propriamente parlando» [Bell 1937, trad. it. p. 529], ma *un insieme* di numeri. Questa è la ragione per cui la nozione dedekindiana di ideale ha messo in ombra la precedente nozione di «ideale» elaborata a suo tempo da Kummer al punto che, comunemente, le usuali storie della matematica sorvolano sugli ideali di Kummer in quanto «superati» da quelli di Dedekind [cfr. per tutti *ibid.*, p. 520]. Ma in questa sede, poiché della nozione di numero si tratta, sarà bene sottolineare che, al contrario che per Dedekind, per Kummer gli ideali erano *numeri*, allo stesso titolo che erano «numeri» i numeri reali o i numeri complessi per Bombelli o per Cataldi, o addirittura per Cavalieri o Torricelli, ai tempi della grande algebra italiana o degli esordi della «geometria degli indivisibili».

«In una memoria di Kummer, – si legge in Ellison [1978, p. 296], che dedica

invece non poche pagine a un'esposizione delle idee originali di Kummer in materia, – Kummer tenta di giustificare la... esistenza [dei numeri ideali] per analogia con una teoria chimica dei radicali ai nostri giorni completamente superata; ma, in fin dei conti, la giustificazione ultima per la loro introduzione è che sono utili e conducono a teoremi matematici significativi. Indipendentemente dalla loro utilità, si trovano negli autori dell'epoca frasi sconcertanti come questa: "I numeri ideali non hanno esistenza quantitativa, ma un numero ideale, elevato a una certa potenza, è eguale a un numero complesso ben determinato"». Non manca, anche in Ellison, il giudizio del senno di poi circa le «idee confuse» di Kummer «superate» dai matematici successivi [*ibid.*, p. 196 in particolare]. In un certo senso, è naturale che, anche per le «tensioni» cui il concetto di numero è stato via via sottoposto, le cose vadano cosí: per dirla con Kuhn [1962], che riecheggia Whitehead, «una scienza che esita a dimenticare i suoi fondatori è perduta» (trad. it. p. 169).

Ma a giustificazione del punto di vista di Kummer per cui i *suoi* ideali erano *numeri* si può invocare il fatto che si sono pure chiamati numeri (reali) le sezioni di Dedekind o le successioni di Cantor, che sono insiemi infiniti di numeri (razionali); ma, mentre i «numeri ideali» di Kummer erano da questi e dal suo allievo Kronecker introdotti *via* la considerazione di un numero finito di congruenze [cfr. Ellison 1978, p. 197], per i «numeri reali» definiti come sezioni o successioni «interviene... un'idea assolutamente nuova, e cioè il concetto di legge (nella teoria di Cantor), ovvero quello di classe, o proprietà (nella teoria di Dedekind)» [Waismann 1936, trad. it. p. 236].

5.4. Un esempio tratto dalla teoria analitica degli ideali.

Nel suo VIII problema Hilbert, accanto ai vari «problemi circa i numeri primi», aggiunge «un problema che... sembra forse di un'importanza ancora piú notevole...: *Trasportare i risultati ottenuti per la distribuzione dei numeri primi alla teoria della distribuzione degli ideali primi di un dato corpo K*» [1900, trad. ingl. p. 17].

La teoria dei numeri primi funziona da paradigma: in perfetta analogia, nel contesto dei numeri algebrici si tratta infatti di trovare una formula asintotica per il numero degli ideali primi $\mathfrak{p}$ di K di norma inferiore a x, ove la norma $N(\mathfrak{p})$ non è altro che il numero finito degli elementi di $O_K/\mathfrak{p}$. Detto $\pi_K(x)$ tale numero, la congettura immediata è $\pi_K(x) \sim (x/\log x)$ (o «teorema» degli ideali primi). L'analogia tra ideali e numeri è dunque, come si vedrà tra poco, euristicamente promettente.

Dedekind introduce, riprendendo ancora una volta uno spunto di Kummer, la nozione di *classe di ideali*. Per *ideali interi* si dice che $\mathfrak{a}$ è equivalente ad $\mathfrak{a}'$ e si scrive $\mathfrak{a} \sim \mathfrak{a}'$ se esiste un ideale $\mathfrak{m}$ tale che $\mathfrak{a}\mathfrak{m}$ e $\mathfrak{a}\mathfrak{m}'$ siano entrambi ideali principali. Se A è la classe di $\mathfrak{a}$ e B quella di $\mathfrak{b}$, si possono moltiplicare le classi di ideali definendo come prodotto AB la classe di $\mathfrak{a}\mathfrak{b}$: per tale operazione le classi di ideali formano un gruppo commutativo finito $H(K)$: l'ordine di $H(K)$, indicato abitualmente $h(K)$, dà notoriamente informazioni sull'«aritmetica» di

O_K. Per $h(K)=1$ ogni ideale intero di K è principale, il che vuol dire che O_K è a fattorizzazione unica.

Ciò premesso, il passo successivo è l'individuazione di un soddisfacente analogo della zeta di Riemann. Si consideri, per s reale >1, la

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} \tag{4}$$

ove la somma va estesa a tutti gli ideali interi $\mathfrak{a}$ di K e $N(\mathfrak{a})$ è la norma dell'ideale $\mathfrak{a}$ definita da $D(\mathfrak{a}) = D_K \cdot N(\mathfrak{a})^2$ e $N(\mathfrak{a}) > O$ (ove $D(\mathfrak{a})$ è definito analogamente a D_K come indicato a p. 935). Ora, come la funzione $\zeta(s)$ di Riemann poteva venir utilizzata per studiare i primi, cosí il comportamento della funzione $\zeta_K(s)$, detta poi zeta di Dedekind, dà informazioni sul numero delle classi $h(K)$ e quindi sull'aritmetica di K. Cosí si deve ancora a Dedekind la formula

$$\lim_{s \to 1+} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R_K}{W\sqrt{|D_K|}}\, h(K) \tag{5}$$

ove D_K è il discriminante (cfr. p. 935) di K, $h(K)$ il numero delle classi, W il numero delle radici dell'unità in K, R_K il cosiddetto regolatore di K (che è una costante che dipende solamente dai generatori del gruppo delle «unità» di O_K), r_1 è il numero delle immersioni canoniche di K in $\mathbf{R}$ e 2^{r_2} il numero delle immersioni canoniche di K in $\mathbf{C}$. È servendosi della funzione zeta che Dedekind ritrova la formula di Kummer per il numero delle classi di un corpo ciclotomico e la stima effettuata da Dirichlet del numero di classi di un corpo quadratico.

Inoltre, come si è già accennato, la dimostrazione del teorema dei numeri primi si basa essenzialmente sulle proprietà della zeta di Riemann: è dunque naturale pensare che la dimostrazione del teorema degli ideali primi dipenda da proprietà analitiche della funzione zeta di Dedekind. L'unico ostacolo era che ancora nel 1896 non si sapeva ancora se $\zeta_K(s)$ ammetteva o no un prolungamento analitico a tutto il piano. Solo nel 1903 Landau mostra che la si può prolungare analiticamente al semipiano $\mathrm{Re}(s) > 1 - 1/[K-\mathbf{Q}]$ e riesce a dimostrare il teorema degli ideali primi. Sono i metodi ivi usati che consentono quindi la dimostrazione semplificata del teorema dei numeri primi di cui a p. 930.

6. *Alcuni aspetti del punto di vista attuale in teoria dei numeri.*

6.1. Corpi locali, adeli, ideli.

Non è certo scopo del presente articolo delineare, seppur brevemente, il punto di vista attuale in teoria dei numeri. Ma poiché tale punto di vista è affrontato in altri articoli della presente *Enciclopedia* con molti dettagli tecnici, sarà qui possibile accennare a ciò che tali sviluppi significano nella prospettiva di un approfondimento della nozione di numero e delle sue proprietà. Come nel paragrafo precedente, il punto di partenza è un corpo K di numeri algebrici, di dimensione n sul corpo $\mathbf{Q}$ dei razionali.

Come si è osservato in altri articoli dell'*Enciclopedia* (cfr. in particolare l'articolo «Divisibilità», vol. V, § 5), la generalizzazione a K di una delle piú familiari nozioni del calcolo, quella di valore assoluto (per cui cfr. «Calcolo», vol. II, pp. 396 e 443), e la conseguente distinzione di valori assoluti *ultrametrici* (tali cioè che $|x+y| \leq \sup(|x|,|y|)$) e *archimedei* (tali cioè che per ogni x, y di K con $x \neq 0$ esiste un numero naturale m tale che $|mx| > |y|$), comportano fondamentali sviluppi di tipo topologico (nozioni esposte in «Geometria e topologia», vol. VI, in particolare pp. 656 sgg. saranno qui presupposte) che coinvolgono alcune non banali generalizzazioni della nozione stessa di numero. Infatti: se si passa da K al suo completato $\hat{K}$ rispetto a valori assoluti archimedei (che sono in numero finito) si ritrova o il corpo $\mathbf{R}$ o il corpo $\mathbf{C}$. Nulla di nuovo sotto il sole: si tratta delle cosiddette *immersioni* canoniche reali o complesse già richiamate nella formula (5) di p. 939. (Se ancora si indica con r_1 il numero delle immersioni reali e con $2r_2$ il numero di quelle complesse vale $r_1+r_2=n$). Ma se l'operazione di completamento (sostanzialmente ricalcata sul classico procedimento di Cantor che permette di «generare» dai razionali $\mathbf{Q}$ i reali $\mathbf{R}$ completando rispetto all'usuale valore assoluto) viene invece svolta a partire da un valore ultrametrico (ve ne è un numero infinito) il corpo $\hat{K}$ che per ciascuno di tali valori si ottiene risulta estensione di grado $\leq n$ di un corpo $\mathbf{Q}_p$ di numeri p-adici (per i quali si rimanda all'articolo «Divisibilità», vol. V, pp. 34 sgg.). Ma giova ricordare che i «numeri» p-adici, introdotti originariamente da Hensel (1908), sono espressione della forma $\sum_{i=r}^{\infty} a_i p^i$ con p primo, $a_r \neq 0$, $r \in \mathbf{Z}$, $a_i \in \mathbf{Z}$, $0 \leq a_i < p$ che «in generale non hanno valore come numeri usuali e però per definizione sono enti matematici» [Kline 1972, p. 1147]. La loro considerazione come numeri e il passaggio ai corpi completati $\hat{K}$ rispetto a valori ultrametrici sono un'ulteriore articolazione del paradigma costituito dal completamento di uno spazio (metrico), paradigma che ha avuto gran peso nello studio sia di spazi numerici sia di spazi di funzioni, ecc. «L'insieme dei concetti (o oggetti) che un linguaggio (o modellizzazione) permette di rappresentare può venir "completato", in certi casi, dai concetti (o oggetti) che questo linguaggio (o modellizzazione) permette di "approssimare indefinitamente". Questi elementi ottenuti per completamento aspirano dunque, irresistibilmente, all'esistenza» [Vallée 1979, p. 28]. Cosí, chiedersi se elementi di $\hat{K}$ siano numeri è ancora una volta come chiedersi [cfr. Waismann 1936, cap. XIV] se i numeri reali definiti alla Cantor siano numeri o no. Quest'ultima definizione, cosí fondamentale da giustificare rigorosamente l'usuale scrittura degli irrazionali come decimali infiniti [cfr. *ibid.*, trad. it. pp. 211 sgg. in particolare] diventa problematica ogni volta che una determinata prospettiva «epistemologica» tende a escludere come illegittimo il procedimento con cui tali nuovi enti sono introdotti. Ma, in sé, tali enti «sono degli inosservabili, per cosí dire, ma non degli inesistenti: un cambiamento di linguaggio [cioè di ontologia] può permettere infatti una loro rappresentazione o una loro approssimazione» [Vallée 1979, p. 28]. Che tipo di raffinamento matematico sottenda tali cambiamenti di linguaggio (o di ontologia) può venir esemplificato non solo da questioni di teoria dei numeri, ma anche in altri contesti

matematici (si pensi, per esempio, alla ricerca di soluzioni di certe equazioni differenziali alle derivate parziali in opportuni completamenti di spazi prehilbertiani di funzioni «ammissibili» come soluzioni del problema originario [cfr. Courant 1950]).

Comunque, quale sia la particolare «filosofia» che nel contesto qui esaminato inquadra questo modo di procedere, la sua rilevanza e la sua capacità di sintesi emergono indiscutibilmente. «I valori assoluti ultrametrici sono quelli che svolgono il ruolo piú importante nelle questioni di *divisibilità*; i valori assoluti archimedei, al contrario, predominano nelle questioni di *approssimazione diofantina*, di *geometria* dei numeri e nello studio dei *numeri trascendenti*. Ma i risultati piú profondi si possono ottenere solo tenendo conto *insieme* dei due tipi di valori assoluti, il che si esprime nella concezione fondamentale degli *adeli* e *ideli*» [Dieudonné 1977, p. 153].

Come il lettore può vedere in «Divisibilità» (vol. V, p. 36 in particolare), a ogni elemento di K si può associare il vettore in cui ogni componente è data dal corrispondente dell'elemento in $\hat{K}$, per ogni valore assoluto. L'idea base, dovuta a Chevalley (1936 e 1940), è stata quella di sostituire alle immersioni di K nei vari corpi locali $\hat{K}$ un opportuno anello A_K o *anello degli adeli* costituito da quei vettori le cui componenti sono ottenute, salvo un numero finito, considerando valori ultrametrici. Le «unità» (elementi invertibili) di A_K sono poi dette ideli. Il fatto essenziale è allora che A_K può venir dotato d'una topologia compatibile con la sua struttura di anello e risultare localmente compatto. Quanto agli ideli essi formano un gruppo moltiplicativo $K_A^\times$ ancora localmente compatto per una topologia piú fine di quella indotta dalla topologia definita sugli adeli.

6.2. Funzioni zeta e funzioni L. Una sintesi.

In questo sofisticato contesto topologico trova adeguata sistemazione proprio la teoria «classica» dei numeri algebrici (cfr. § 5), come il lettore può constatare consultando l'elegante e sintetica esposizione di Dieudonné [1977, in particolare p. 155]. Ma il fatto che il gruppo degli ideli sia un gruppo commutativo localmente compatto rende possibile anche un'applicazione dei risultati dell'analisi armonica che consente un'esposizione unitaria e semplificata della teoria classica delle funzioni zeta e delle funzioni L. È questa oggi, forse, «l'applicazione piú inattesa» [*ibid.*, p. 216] di uno strumento tipico dell'analisi.

Anche in tale contesto si presupporranno, nel delineare brevemente questo tipo di approccio, nozioni ampiamente trattate in altri articoli dell'*Enciclopedia* (in particolare «Dualità», vol. V, pp. 173 sgg., e «Invariante», vol. VII, pp. 925 sgg.). Cosí sul gruppo degli ideli si definisce una misura di Haar privilegiata (usualmente detta misura di Tamagawa) rispetto a cui il secondo membro della formula di Dedekind (5) del § 5 risulta un invariante dotato di particolare significato geometrico. Tate ha quindi definito (1951) una funzione zeta generale

$$\zeta(f,c) = \int_{K_A^\times} f(z)\, c(z)\, d^\times z$$

ove l'integrazione, rispetto alla misura in questione, è fatta sul gruppo degli ideli: f è una funzione su A_K che verifica certe condizioni di regolarità (come anche la sua trasformata di Fourier) e c è un «quasi carattere», cioè un omomorfismo continuo del gruppo detto delle *classi di ideli* C_K (ottenuto come quoziente del gruppo degli ideli modulo il gruppo moltiplicativo del corpo K, cioè $K-\{0\}$): si tratta di una generalizzazione della nozione di carattere, dovuta a Hecke (1918-20).

La teoria di questa nuova funzione zeta compendia sia quella della zeta di Riemann (prendendo per K il corpo $\mathbf{Q}$) sia quella delle funzioni L variamente generalizzate. Esprime dunque, in modo estremamente sintetico, questioni di teoria dei numeri primi (cfr. § 4) e questioni di teoria degli ideali primi (cfr. § 5) unificando due trattazioni che si è visto procedere pressoché parallelamente, ma in modo distinto.

L'interesse delle funzioni L sta soprattutto nelle relazioni che forniscono informazioni sui numeri $h(K)$ e R_K. Il risultato piú notevole in questa direzione si deve a Siegel: se per una successione infinita di corpi di numeri algebrici K è $\lim n \log(D_K)=0$ si ha allora $\log h(K)R_K \sim \log\sqrt{|D_K|}$. Per le estensioni quadratiche $K=\mathbf{Q}(\sqrt{d})$ di $\mathbf{Q}$, ove $d=D_K$ la considerazione delle funzioni L aveva condotto a suo tempo Dirichlet (cfr. p. 929) a formule esplicite per $h(K)$. Il teorema di Siegel ha permesso di mostrare che per $d<0$ esiste solo un numero finito di valori di d per cui h è fissato. È in particolare finito il numero dei corpi K per cui $h(K)=1$ (cioè per cui ogni ideale è principale): di recente si è riusciti a determinare esplicitamente tutti tali corpi (sono in tutto *nove*, per $-d=1, 2, 3, 7, 11, 19, 43, 67, 163$) sfruttando relazioni intercorrenti tra differenti funzioni L, corrispondenti a caratteri χ differenti, e proprietà di approssimazione diofantina legate alla teoria dei numeri trascendenti; gli stessi metodi hanno permesso di determinare i numeri $d<0$ per cui $h(K)=2$ (teoremi di Baker e Stark).

6.3. Corpi locali e corpi globali.

Una teoria analoga si può sviluppare per estensioni algebriche finite dei corpi $\mathbf{F}_q(X)$, corpi delle funzioni razionali su una curva algebrica definita sul corpo finito $\mathbf{F}_q$. Per questi corpi si possono definire tutte le nozioni precedenti: adeli, ideli, funzioni zeta, ecc. e i risultati si estendono con poche modificazioni. Di fatto sono piú semplici a causa dell'assenza dei valori assoluti archimedei: cosí «la geometria algebrica consente spesso di dimostrare delle proprietà di questi corpi che conducono a congetturare proprietà analoghe (generalmente molto piú difficili a dimostrarsi) per i corpi numerici» [Dieudonné 1977, p. 156]. Sotto il nome di *corpi globali* si designano talvolta le estensioni algebriche finite di $\mathbf{Q}$ e di $\mathbf{F}_p(X)$. «Lo studio di tali corpi K è inseparabile da quello dei corpi locali $\hat{K}$ che si ottengono da K completandolo rispetto ai suoi diversi valori assoluti: il modo di procedere seguito nello studio di una questione concernente K consiste nella maggior parte dei casi a "localizzarla" considerandola innanzitutto su un corpo locale; quindi a "globalizzare" i risultati ottenuti per i diversi $\hat{K}$» [*ibid.*, p. 157; si veda anche l'articolo «Locale/globale» in questa stessa *Enciclopedia*, vol. VIII, in particolare pp. 482-85].

6.4. Ipotesi di Riemann per varietà su un corpo finito.

L'influenza della geometria algebrica sulla teoria dei numeri può venir bene messa in luce accennando a un ordine di idee che rappresenta, di nuovo, un'ulteriore generalizzazione del paradigma emerso nella teoria moltiplicativa dei numeri con Riemann [1859]. Come già si è detto in altri articoli della presente *Enciclopedia* (si veda in particolare «Geometria e topologia», vol. VI, pp. 695 sgg.), l'approccio di Hasse e Weil in geometria algebrica ha portato alla formulazione di «ipotesi di Riemann» *per varietà su corpi finiti*. Il senso profondo dei risultati recentemente ottenuti da Pierre Deligne si coglie, ancora una volta, non solo nella potenza degli strumenti geometrico-topologici (coomologia l, cfr. *ibid.*), ma nella retroazione che questi e analoghi risultati hanno sulla teoria dei numeri [cfr. per tali aspetti Bombieri 1976; Katz 1976]. L'originaria ipotesi riemanniana resta ancora non decisa, ma la dimostrazione dei suoi analoghi per corpi finiti e lo spiegamento delle ipotesi «generalizzate» (cfr. p. 932) può costituire la nervatura di una nuova sintesi.

6.5. Elementi per una valutazione complessiva.

«Bisogna anche tener conto del ruolo che hanno svolto i numeri naturali nella maggior parte delle filosofie e delle religioni antiche, e in particolare, nei pitagorici e in tutti gli altri pensatori che hanno subito la loro influenza; questi ultimi non avevano che disprezzo per coloro che volevano infangare con basse preoccupazioni pratiche le gioie della contemplazione del Bello e del Vero che procurano le proprietà dei numeri a coloro che si dedicano al loro studio» [Dieudonné e altri 1978, I, p. 10]. A distanza di piú di un secolo, sembra di risentire un detto di Kummer: la teoria dei numeri «ha per oggetto la matematica stessa, senza riguardo alle sue applicazioni» [citato in Bell 1937, trad. it. p. 521]. E sulle applicazioni della teoria dei numeri nelle sue formulazioni classiche e nell'impostazione attuale c'è chi, drasticamente, conclude: «Nessuna, almeno per il momento!» [valga per tutti Dieudonné 1977, p. 170]. C'è dunque una spaccatura fra l'approfondimento delle proprietà che avvicinano il matematico «puro» odierno, non meno che il pitagorico, «alla contemplazione del Bello e del Vero» e le applicazioni alle scienze empiriche. A parere di chi scrive, l'*utilizzazione* dei risultati di teoria dei numeri nella modellizzazione dei processi reali può emergere solo *per canali molto indiretti*. Sviluppi astratti di una modellizzazione, a prima vista molto naturale (cfr. le osservazioni sviluppate a tale proposito nell'articolo «Modello» di questo stesso volume dell'*Enciclopedia*, in particolare nel § 2), come quelli qui esposti costituiscono il banco di prova di *metodi generali* che investono anche settori delle matematiche piú direttamente coinvolti nella matematizzazione delle scienze empiriche. Sotto questo profilo la sintesi delineata in questo paragrafo è davvero esemplare: teoria dei numeri e,

per esempio, meccanica quantistica diventano *insieme* terreno privilegiato dell'applicazione della analisi armonica. Kummer pensava che i suoi fattori primi ideali rivelassero «l'essenza dei numeri complessi», rendendoli come trasparenti e scoprendo «la loro cristallina struttura intima» [citato in Bell 1937, trad. it. p. 517].

Oggi noi forse non riteniamo piú che, poniamo, l'impiego di certi invarianti rispetto a certe misure (cfr. sopra, pp. 941 sgg.) rivelino una qualche «essenza»; ma possiamo a buon diritto credere che rendere sempre piú «trasparenti» alcune situazioni, siano esse matematiche o empiriche, possa costituire un esempio non banale di progresso scientifico.

7. *Dare «numeri» alle «cose».*

È questa, come qualcuno direbbe, «la posta in gioco»: dalla numerologia pitagorica alla meccanica quantistica (e, ancora una volta, l'accoppiamento non è casuale: cfr. le considerazioni finali dell'articolo «Fisica» in questa stessa *Enciclopedia*). Cosí il basare una porzione rilevante della modellizzazione del reale su relazioni numeriche è stato via via la leva della «rivoluzione galileiana», lo strumento di grandi sintesi scientifiche come quella di Newton (o di Einstein, o di Heisenberg), il segno della maturità di una scienza (Kant, per esempio) o del distacco profondo dal «mondo della vita» (Husserl, Heidegger)... In questo senso teorie scientifiche e metafisiche influenti hanno *giocato con i numeri*, non meno dell'antica *gematria*, tendenza «magica» ad associare ai numeri significati iniziatici. Le riflessioni che seguono mirano a chiarire l'elemento base di questo «gioco», *l'assegnazione di «numeri» a «cose»*. La sfida – proprio come nel caso dei grandi problemi della teoria dei numeri – è contenuta, di nuovo, in una tesi che Aristotele attribuisce ai pitagorici: «Pareva loro evidente che tutte le altre cose modellassero sui numeri la loro intera natura e che i numeri fossero l'essenza primordiale di tutto l'universo fisico; e per tutte queste ragioni essi concepirono gli elementi dei numeri come elementi di tutta la realtà, e l'intero cielo come armonia e numero» [*Metafisica*, 985b, 33 - 986a, 3].

Come negli sviluppi astratti considerati nei paragrafi precedenti si è rivelato cruciale il progressivo slittamento dalla successione dei naturali al continuo lineare **R** o al continuo bidimensionale **C**, anche nella «aritmetizzazione» delle situazioni empiriche che viene esaminata in questo paragrafo l'estensione dal caso dei naturali **N** ai reali **R** e ai complessi **C** solleva piú di un problema. Quando si passa dalla semplice assegnazione di numeri naturali a collezioni finite di oggetti ai casi piú complicati, tipo misurazione di masse, lunghezze, ecc., emerge questo primo problema: che cosa giustifica questo modo di procedere, che conferisce ai numeri un ruolo privilegiato come strumento di comprensione della natura?

D'altra parte, tali assegnazioni numeriche non sono in generale uniche: un unico numero intero rappresenta la cardinalità di una collezione finita di oggetti, ma quale numero reale rappresenti la lunghezza di una pertica dipende

dalle unità di misura fissate! Secondo problema dunque: che relazioni sussistono tra i diversi numeri che rappresentano – entro diversi sistemi di misura – una stessa proprietà o relazione empiricamente determinabile?

7.1. Il primo problema fondamentale.

Un abbozzo di risposta al primo problema sta già nell'idea pitagorica secondo cui ogni cosa «modella la sua natura sui numeri». Un modo di interpretare questa affermazione consiste nel sostenere che certe situazioni empiriche *hanno la stessa struttura* di certi sistemi numerici. I termini cruciali di questa reinterpretazione sono ovviamente tre: 'situazione empirica', 'avere la stessa struttura' e 'sistema numerico'.

Si presupporranno qui alcuni concetti base della teoria degli insiemi (si veda del resto l'articolo «Insieme» in questa stessa *Enciclopedia*). In questo contesto, si può identificare una «situazione empirica» con un *sistema relazionale*, e cioè con un insieme di oggetti su cui sono definite certe proprietà e relazioni, che nel caso dovranno risultare empiricamente determinabili. Potrebbe per esempio trattarsi di un insieme di eventi e della relazione «x è almeno tanto probabile di y, per il soggetto X». Piú formalmente un sistema relazionale (finitario) è una sequenza finita della forma $\mathbf{A} = \langle A, R_1, ..., R_n \rangle$ dove A è un insieme non-vuoto di elementi detto *dominio* del sistema relazionale, e $R_1, ..., R_n$ sono relazioni definite su A. Il sistema relazionale **A** è detto finito se A è finito; altrimenti infinito. Dal nostro punto di vista, un sistema relazionale non è che la codificazione insiemistica di certi dati empirici di carattere qualitativo concernenti la questione se date relazioni sussistono o meno tra opportune sequenze di oggetti del dominio del sistema relazionale considerato. Si dice inoltre *tipo* di un sistema relazionale la sequenza finita di numeri naturali la cui lunghezza è pari al numero di relazioni appartenenti al sistema relazionale e al cui i-esimo posto sta l'intero che rappresenta il numero di posti della relazione R_i appartenente al sistema relazionale.

Per sistema numerico si intenderà qui semplicemente un sistema relazionale il cui dominio è costituito dall'insieme dei numeri reali o da un suo sottoinsieme.

Infine, dati due sistemi relazionali, $\mathbf{A} = \langle A, R_1, ..., R_n \rangle$, di tipo $\langle m_1, ..., m_n \rangle$, e $\mathbf{B} = \langle B, S_1, ..., S_n \rangle$, dello stesso tipo, si dice che hanno la stessa struttura, o che sono *isomorfi*, se e solo se esiste una funzione biunivoca f da A su B tale che $R_i x_1 ... x_{m_i}$ se e solo se $S_i f(x_1) ... f(x_{m_i})$, per $i = 1, 2, ..., n$.

La condizione che f sia biunivoca è però troppo restrittiva agli effetti del nostro problema; accade infatti spesso che a *piú* oggetti venga assegnato *uno stesso* numero. Conviene perciò disporre di una nozione piú generale che si ottiene lasciando cadere il requisito che f sia biunivoca. In tal caso, si dice che i due sistemi relazionali sono *omomorfi*.

La natura sarà perciò davvero fatta ad immagine dei numeri in tutti e soli quei casi in cui esiste un omomorfismo tra una data classe di sistemi relazionali (empirici) e un appropriato sistema numerico. È questo il cosiddetto «problema della rappresentazione» per una data classe di sistemi. La sua soluzione positiva

– un teorema di rappresentazione – fa di questa classe una *teoria della misurazione*, giustificando l'assegnazione di numeri alle proprietà e relazioni coinvolte.

Il problema della rappresentazione risulterebbe matematicamente banale se *qualunque* classe di sistemi relazionali (di uno stesso tipo, chiusa rispetto ad isomorfismi) fosse una teoria della misurazione, ammettesse cioè un omomorfismo in un sistema numerico. Un semplice controesempio stabilirà che questo non è il caso. Sia **K** la classe di tutti i sistemi relazionali di tipo $\langle 2 \rangle$ che sono ordinamenti semplici, tali cioè che R è antisimmetrica, transitiva e fortemente connessa. Sia $\langle A, R \rangle$ un elemento di **K**, tale che R bene ordina A, tale che cioè ogni sottoinsieme non-vuoto di A ha un primo elemento rispetto alla relazione R, e A ha una cardinalità che non sia uguale o minore a quella del continuo. Si supponga allora, per assurdo, che **K** sia una teoria della misurazione rispetto al sistema numerico $\langle$Reali, $S \rangle$, dove S è una relazione binaria arbitraria. Dalla definizione di teoria della misurazione segue che esiste una funzione f da A su (un sottoinsieme) dell'insieme dei reali tale che Rxy se e solo se $Sf(x)f(y)$, per tutti gli x e y di A. Siano a e b due elementi di A tali che $f(a)=f(b)$. Dato che R è un ordinamento semplice, vale o che Rab oppure che Rba. Si assuma che valga Rab. Ne segue che $Sf(a)f(b)$, e dato che per ipotesi $f(a)=f(b)$, anche che $Sf(b)f(b)$, e infine che Rba. Ma R è antisimmetrica, dunque $a=b$. Questo implica che f è biunivoca e quindi che A ha la stessa potenza di un sottoinsieme dell'insieme dei reali, il che contraddice la nostra ipotesi che A ha una potenza che non è minore o uguale a quella del continuo.

Ma che succede se si restringe **K** alla classe **K**′ che contiene solo sistemi al massimo numerabili – caso che di fatto si verifica nella pratica della codificazione di dati empirici qualitativi? Si può dimostrare allora che esiste sempre un omomorfismo f del tipo richiesto. La ragione per cui questo risultato non banalizza da un punto di vista empirico il problema della rappresentazione è che il sistema numerico richiesto per ottenerlo è cosí «patologico» da non essere di alcuna utilità computazionale. Infatti, non appena si pongono su di esso alcune restrizioni del tutto naturali in vista dello scopo principale dell'assegnazione di numeri a proprietà e relazioni empiriche, e cioè la disponibilità di efficienti strumenti di calcolo, non sempre esistono omomorfismi appropriati.

In queste circostanze, il problema della rappresentazione diventa il problema di quali caratteristiche debbono godere date proprietà e relazioni empiriche per poter essere rappresentate numericamente in modo «naturale». Per quanto, contrariamente a un'opinione assai diffusa, vi siano vari sistemi di caratteristiche che consentono tale rappresentazione, non sono correntemente noti molti metodi di costruzione di omomorfismi appropriati, di omomorfismi cioè che consentano l'immersione di sistemi relazionali empirici in sistemi numerici «naturali», almeno se ci si limita a prendere in considerazione i metodi «fondamentali», che non dipendono cioè da precedenti assegnazioni numeriche. Per esempio, la lunghezza ammette un metodo di misurazione fondamentale, mentre la densità dipende per la propria misurazione da una precedente misurazione di massa e volume, essendo definita come il rapporto fra massa e volume. Di tali metodi fondamentali ne sono stati distinti essenzialmente tre.

a) *Assegnazioni numeriche ordinali.* In questo caso ci si aspetta dai numeri che codifichino solo l'ordine di un dato insieme di oggetti rispetto a una data proprietà empirica. Un esempio noto è la scala di Mohs per la durezza dei minerali. Eccone una «ricostruzione razionale» che mette bene in luce le sue caratteristiche concettualmente salienti. Si fissi come A un certo insieme di minerali, e come R la relazione «x è piú duro di y». Per rendere empiricamente determinabile questa relazione, Mohs propose di definirla nel modo seguente: x è piú duro di y se e solo se x scalfisce y. Si fissi ora come sistema numerico l'insieme dei reali con l'usuale relazione di maggiore. Un modo ovvio per costruire un omomorfismo f appropriato è: si sceglie un minerale a caso e gli si assegna un numero arbitrario. Se ne sceglie un secondo, e si controlla quale dei due scalfisce l'altro. Se il primo scalfisce il secondo, si assegna a quest'ultimo un qualsivoglia numero minore, e se il secondo scalfisce il primo, un qualsivoglia numero maggiore. Con il terzo si procede allo stesso modo, salvo nel caso in cui scalfisca uno dei due precedenti e sia scalfito dall'altro; in questo caso gli si assegna un numero arbitrario tra i due precedentemente assegnati. Non è difficile vedere che questa procedura può essere continuata indefinitamente, senza che le precedenti assegnazioni debbano essere riviste alla luce delle successive, grazie alla densità dell'insieme dei reali.

Una difficoltà che si potrebbe incontrare in questo caso è che potrebbero esservi due minerali a e b tali che né a scalfisce b né b scalfisce a. Una possibilità naturale sarebbe di concludere allora che a e b sono ugualmente duri ed assegnare ad essi lo stesso numero. Tuttavia, se il test è insensibile a piccole differenze di durezza, ci si potrebbe trovare di fronte a tre minerali a, b e c, tali che a sia duro tanto quanto b, b tanto quanto c, ma a piú duro di c, il che escluderebbe l'esistenza di un omomorfismo. Test di questo genere per la misurazione ordinale sono perciò appropriati quando la loro sensibilità è maggiore delle differenze tra i minerali sotto esame. Tuttavia, perché la funzione f cosí definita costituisca davvero un omomorfismo, la relazione «x scalfisce y» deve godere di certe caratteristiche formali. Deve, per esempio, essere transitiva. Si supponga infatti che non lo sia. Si potrebbero allora avere tre minerali a, b e c tali che a scalfisca b, b scalfisca c, ma c scalfisca a. Si avrà allora, in base alla definizione di f, $f(a)>f(b)>f(c)>f(a)$, il che è impossibile. È perciò una delle difficoltà principali, quando si vogliono assegnare numeri a proprietà e a relazioni empiriche, quella di interpretarle in modo tale che esse godano – di fatto – delle caratteristiche formali che consentano un omomorfismo del tipo voluto. È precisamente questo il cosiddetto «problema dell'assiomatizzazione»: quali caratteristiche formali debbono essere soddisfatte dalle proprietà e relazioni empiriche considerate perché esista un omomorfismo del tipo voluto? Si illustrerà questo problema con un esempio semplice. Come d'uso, per A insieme e R relazione binaria su A, si dice che $\langle A, R \rangle$ è un *ordine debole* se e solo se, per tutti gli $x, y, z \in A$, vale: 1) Rxy o Ryx; 2) se Rxy e Ryz, allora Rxz. L'insieme dei reali con l'usuale relazione di $\leq$ è un ordine debole, che soddisfa inoltre la condizione: se Rxy e Ryx, allora $x=y$. Un ordine debole che soddisfa anche que-

sta condizione viene detto semplice o totale. Si può allora dimostrare il seguente teorema:

TEOREMA DI RAPPRESENTAZIONE (Krantz, Luce, Suppes, Tversky). *Sia A un insieme non-vuoto finito e $\langle A, R\rangle$ un ordine debole. Esiste allora una funzione f a valori reali tale che per ogni $x, y \in A$, Rxy se e solo se $f(x) \leq f(y)$.*

Questo teorema stabilisce dunque che la classe di tutti gli ordini deboli finiti è una teoria della misurazione relativamente al sistema numerico $\langle$Reali, $\leq\rangle$. La sua dimostrazione esemplifica una delle tecniche principali per dimostrazioni di esistenza di omomorfismi, e inoltre illustra la relazione tra assiomi e procedure di misurazione. Essa dà anche un metodo per costruire un omomorfismo del tipo voluto, metodo che costituisce precisamente la procedura di misurazione.

Il primo passo consiste nell'associare all'ordine debole dato un ordine semplice, identificando tutti gli elementi di A tali che Rxy e Ryx. A partire da R, si definisce perciò una nuova relazione, I, nel modo seguente: Ixy se e solo se Rxy e Ryx. Non è difficile dimostrare che I è una relazione di equivalenza. Si può perciò formare l'insieme quoziente di A rispetto a I, A/I, e denotare la classe di equivalenza determinata da $y \in A$, con $[y]$. L'ordine debole R induce allora un nuovo ordine R' su A/I ponendo: $R'[x][y]$ se e solo se Rxy. È facile dimostrare che R' è un ordine semplice.

Ora, se la funzione f del teorema esiste, essa deve necessariamente assegnare lo stesso valore a tutti gli elementi di una data classe di equivalenza. Si supponga infatti che Ixy; allora Rxy e Ryx; dunque $f(x) \leq f(y)$, e $f(y) \leq f(x)$, che implica $f(x) = f(y)$. Nella costruzione di f ci si deve preoccupare semplicemente del fatto che essa rispetti l'ordine tra le varie classi. Basterà perciò costruire una F dall'insieme-quoziente nell'insieme dei reali tale che $R'[x][y]$ se e solo se $F([x]) \leq F([y])$. La f voluta risulterà determinata allora ponendo $f(x) = F([x])$.

Questo riduce il problema della rappresentazione per gli ordini deboli a quello per gli ordini semplici. Si definisce allora $F([x])$ ponendolo uguale al numero di classi di equivalenza $[y]$ tali che $R'[x][y]$, che cioè precedono $[x]$ rispetto a R'. Si noti che la condizione di finitezza è essenziale perché questa definizione abbia senso. Infatti, essa implica che tali classi sono necessariamente in numero finito.

Non è difficile, infine, verificare che F è un omomorfismo.

Questo teorema si estende senza difficoltà agli ordini semplici numerabili, semplicemente raffinando il metodo di costruzione delineato per la scala di Mohs.

Si è detto che un teorema di rappresentazione giustifica l'assegnazione di numeri a ben specificate situazioni empiriche. In generale, tuttavia, non giustifica affatto un'interpretazione «essenzialistica» di tale assegnazione, in base alla quale i numeri assegnati catturerebbero l'intera essenza della proprietà o relazione empirica misurata. Nel caso di assegnazioni numeriche ordinali sarebbe per esempio del tutto fallace concludere, dal fatto che, sotto un particolare omomorfismo, un minerale a ha una durezza pari a 10 e un minerale b pari a 100, che il secondo è 10 volte piú duro del primo. La ragione è che tale omomorfismo non è unico, ovvero che tali numeri sono del tutto arbitrari eccetto che per la loro proprietà di conservare l'ordine degli oggetti considerati rispetto alla proprietà o relazione empirica considerata.

b) Assegnazioni numeriche basate sul conteggio delle unità. Se su un insieme di oggetti risulta definita non solo una relazione d'ordine, ma inoltre un'operazione di «concatenazione», diventa allora possibile pensare agli oggetti considerati come costituiti da un certo numero di «unità» ed utilizzare questo numero come misura della proprietà corrispondente alla relazione d'ordine considerata. È proprio questo il modo di procedere usuale con grandezze come la massa, la lunghezza, ecc. Si veda l'esempio della lunghezza. In questo caso A è un insieme di pertiche rigide e diritte, e R è relazione «x è piú lunga di y». Ovviamente, si dirà che x è piú lunga di y se, una volta sovrapposte in modo che coincidano a una delle loro estremità, x si estende oltre y all'altra estremità. Nel caso in cui coincidano anche all'altra estremità, si dirà invece che hanno la stessa lunghezza. Fino a questo punto, si ha a che fare con un ordine debole. Non è però difficile definire in questo caso un'operazione di concatenazione. Si dirà che la pertica z è il concatenato delle pertiche x e y se z è la pertica che risulta disponendo x e y in linea retta estremità a estremità, e si denoterà z con «$x \circ y$». Data questa interpretazione dell'operazione di concatenazione, è intuitivamente chiaro che eventuali assegnazioni numeriche dovranno soddisfare condizioni addizionali rispetto a quella precedentemente considerata. Siano per esempio a_1, a_2, a_3, ... copie perfette l'una dell'altra, e si supponga valido che $a_1 \circ a_2$ è piú lungo di b e che b è piú lungo di a_1. Come prima, ci si aspetta che f sia tale che $f(a_1 \circ a_2) > f(b) > f(a_1) = f(a_2)$, ma ora ci si aspetta anche che $f(a_1 \circ a_2) = f(a_1) + f(a_2) = 2f(a_1)$.

Anche in questo caso, il problema è quello di determinare di quali caratteristiche debbano godere la relazione R e l'operazione di concatenazione perché esista un omomorfismo del tipo voluto. Si considera qui il caso dei cosiddetti sistemi estensivi. Innanzitutto, un sistema estensivo è un sistema relazionale $\langle A, R, \circ\rangle$, in cui R è una relazione binaria, $\circ$ è un'applicazione di $A \times A$ ad A che soddisfa le seguenti condizioni per tutti gli x, y e z in A:

1) Se Rxy e Ryz, allora Rxz.
2) $R((x \circ y) \circ z)(x \circ (y \circ z))$.
3) Se Rxy, allora $R(x \circ z)(z \circ y)$.
4) Se non Rxy, allora esiste uno z in A tale che $Rx(y \circ z)$ e $R(y \circ z)x$.
5) Non si dà il caso che $Rx(x \circ y)$.
6) Sia nx definito induttivamente nel modo seguente:
   a) $1x = x$
   b) $(n+1)x = nx \circ x$.
   Se Rxy, allora esiste un n tale che $Ry(nx)$.

1)-6) implicano in particolare che R è un ordine debole. La sua interpretazione nel caso della lunghezza è «x è meno lungo di y oppure ha la stessa lunghezza

di y», dato che è tecnicamente piú semplice lavorare con questa relazione piuttosto che con quella prima considerata «x è piú lungo di y». L'interpretazione dell'operazione di concatenazione resta invece la stessa.

Se a questo punto si sceglie come sistema numerico l'insieme dei reali positivi con l'usuale relazione d'ordine e operazione di addizione, si è in grado di dimostrare il seguente

TEOREMA DI RAPPRESENTAZIONE. *Se $\langle A, R, \circ\rangle$ è un sistema estensivo, allora esiste una funzione f da A dei reali positivi tale che per tutti gli x e y in A:*

1) *Rxy se e solo se $f(x) \leq f(y)$;*
2) *$f(x \circ y) = f(x) + f(y)$.*

L'idea della sua dimostrazione (Krantz, Luce, Suppes, Tversky) – che qui non viene riportata – consiste nella sua riduzione a un teorema di Hölder (1901) concernente i gruppi archimedei semplicemente ordinati. Il passo principale della riduzione consiste di nuovo nella definizione di un'opportuna relazione di equivalenza su $A \times A$: $I'(x,y)(w,z)$ se e solo se $I(x \circ z)(y \circ w)$, dove Ixy è definito come al solito con Rxy e Ryx. Utilizzando I', è allora possibile costruire un nuovo sistema relazionale che risulta un gruppo archimedeo semplicemente ordinato.

Il teorema stabilisce allora che la classe di tutti i sistemi estensivi è una teoria della misurazione rispetto all'insieme dei reali positivi con l'usuale ordinamento e operazione di addizione. Fortunatamente esso può essere generalizzato in varie direzioni in modo da renderlo applicabile ai sistemi estensivi con cui si ha effettivamente a che fare nella pratica. La generalizzazione piú interessante da questo punto di vista riguarda il caso di quei sistemi in cui l'operazione di concatenazione non è definita su tutto A.

c) Assegnazioni numeriche basate sulla soluzione di diseguaglianze. Si supponga di avere a che fare con un sistema estensivo per cui si dispone dei seguenti dati qualitativi, dove $Rsxy$ sta per Rxy e non Ryx: $Rs(x_1 \circ x_5)(x_3 \circ x_4)$; $Rs(x_3 \circ x_4)(x_1 \circ x_2)$; $Rs(x_1 \circ x_2)x_5$; Rsx_5x_4; Rsx_4x_3; Rsx_3x_2; Rsx_2x_1.

Ora, assumendo che un omomorfismo f da questo sistema estensivo in $\langle$Reali positivi, $\leq$, $+\rangle$ esista, si è qui interessati a determinare i valori che esso assegna agli elementi di A considerati. Sia allora r_i il valore (incognito) che esso assegna a x_i, $i = 1, \ldots, 5$. I dati qualitativi precedenti determinano allora il seguente sistema di diseguaglianze lineari:

$$\begin{cases} r_1 + r_5 - r_3 - r_4 > 0 \\ r_3 + r_4 - r_1 - r_2 > 0 \\ r_1 + r_2 - r_5 > 0 \\ r_5 - r_4 > 0 \\ r_4 - r_3 > 0 \\ r_3 - r_2 > 0 \\ r_2 - r_1 > 0. \end{cases}$$

Qualunque soluzione di questo sistema in cinque incognite ci darà allora un insieme di valori possibili per $x_1, \ldots, x_5$. Naturalmente, questo metodo può essere generalizzato e risulta particolarmente comodo quando, pur essendo ragionevole assumere l'esistenza di un omomorfismo appropriato, o essendo addirittura in grado di dimostrarla, è troppo complesso mettere in atto una procedura di misurazione basata su sequenze standard.

7.2. Il secondo problema fondamentale.

Si tratta qui di rispondere alla domanda: in che misura una data assegnazione numerica è convenzionale e in che misura invece rispecchia l'«essenza» della proprietà misurata? E inoltre: in quanto un'assegnazione è *convenzionale*, altre assegnazioni saranno ugualmente accettabili. Che relazioni devono sussistere tra queste assegnazioni alternative? Questo punto di vista consente una classificazione particolarmente interessante degli omomorfismi da un sistema relazionale a un sistema numerico. Per usare una terminologia piú familiare, si introdurrà la nozione di scala. Per *scala* si intenderà una tripla costituita da un sistema relazionale, un sistema numerico e una funzione f che stabilisce un omomorfismo tra i due. Diverse scale saranno allora caratterizzate dalla relativa unicità della funzione f, e cioè dalla relazione che sussiste tra i vari omomorfismi dal sistema relazionale dato al sistema numerico dato. Questa nozione può essere resa precisa mediante la nozione di *trasformazione ammissibile*. Si suppongano fissati sia il sistema relazionale **A** sia il sistema numerico, che per comodità si denoterà con **B**. Sia infine $\langle \mathbf{A}, \mathbf{B}, f\rangle$ una scala. Si dice allora che G è una trasformazione ammissibile se e solo se $\langle \mathbf{A}, \mathbf{B}, G(f)\rangle$ è di nuovo una scala.

a) Scale assolute. Le scale assolute sono quelle caratterizzate dall'unicità dell'omomorfismo. Questo implica che la trasformazione ammissibile è quella identica per cui $G(f) = f$. Il contare, l'assegnazione cioè di un numero intero ai membri di un dato insieme finito, è un esempio non controverso di scala assoluta: dato un insieme finito di oggetti, esiste un unico numero intero che rappresenta la sua cardinalità.

b) Scale ordinali. Sono quelle che si situano all'estremo opposto delle scale assolute. Come già si è notato, sono totalmente convenzionali eccetto che per l'ordine. Questo implica che le trasformazioni ammissibili devono essere monotone, devono cioè soddisfare una delle due seguenti condizioni:

1) se $f(x) < f(y)$, allora $G(f(x)) < G(f(y))$, oppure
2) se $f(x) < f(y)$, allora $G(f(x)) > G(f(y))$.

Le scale ordinali vengono perciò dette uniche a meno di trasformazioni monotone.

c) Scale di rapporti. Alcune delle piú importanti scale fisiche sono scale di rapporti, come la scala per la lunghezza, la massa, ecc. In questo caso, la compo-

nente convenzionale è ristretta alla scelta di un'unità di misura, come si è visto nella nostra discussione dei sistemi estensivi. Quel che risulta dunque determinato univocamente sono i rapporti $f(x)/f(y)$. Perciò, se **A** è un sistema estensivo e $\langle \mathbf{A}, \mathbf{B}, f \rangle$ è la scala corrispondente, dove f è un'assegnazione numerica basata sulla scelta di u come unità, e $\langle \mathbf{A}, \mathbf{B}, f' \rangle$ è un'altra scala, dove f' è un'assegnazione numerica basata sulla scelta di u' come unità, si avrà $f(x)/f(u) = f'(x)/f'(u')$, e quindi, dato che $f(u) = 1$, $f(x) = f'(x)/f'(u')$. Ponendo $f(u') = k$, si ottiene allora $f'(x) = kf(x)$. Trasformazioni G tali che $G(f(x)) = kf(x)$, con $k > 0$, vengono dette trasformazioni di similarità. Si dimostra facilmente che se **A** è un sistema estensivo e $\langle \mathbf{A}, \mathbf{B}, f \rangle$ una scala, allora lo è anche $\langle \mathbf{A}, \mathbf{B}, f' \rangle$ se e solo se esiste un $k > 0$ tale che $f'(x) = kf(x)$. Le scale di rapporti sono quindi uniche a meno di trasformazioni di similarità.

d) *Scale di intervalli.* Due esempi importanti di scale di intervalli sono quelle per la temperatura e per l'utilità. In questo caso, la componente convenzionale è costituita non solo dalla scelta di un'unità di misura, ma anche di un'origine. Quel che risulta perciò univocamente determinato sono i rapporti fra intervalli, nel senso che se $\langle \mathbf{A}, \mathbf{B}, f \rangle$ è una scala, allora lo è anche $\langle \mathbf{A}, \mathbf{B}, f' \rangle$, dove:

$$\frac{f'(x) - f'(y)}{f(w) - f'(z)} = \frac{f(x) - f(y)}{f(w) - f(z)}.$$

Trasformazioni che soddisfano questa condizione vengono dette affini e definite come segue: $G(f(x)) = kf(x) + m$, dove $k > 0$. Per esempio la relazione tra la scala Celsius e quella Fahrenheit è determinata dalla seguente trasformazione: $C = (5/9)(F - 32)$.

8. *Invece della conclusione.*

Le questioni delineate nel paragrafo precedente sottendono l'impiego dei numeri come strumento essenziale e di conoscenza e di azione (cfr. «Modello» di questo stesso volume e, ancora, nell'*Enciclopedia*, gli articoli «Dato» e «Misura»): quanto si è trattato negli altri paragrafi (in particolare §§ 4, 5, e 6) concerne soprattutto il ruolo e i nessi fondamentali dei numeri con altri concetti base delle matematiche. I due aspetti spesse volte si sono accavallati (si pensi alle considerazioni dei primi tre paragrafi) facendo emergere insospettate connessioni (per esempio, crisi del pitagorismo concomitante alla scoperta dell'irrazionale, § 2; questioni evidenziate alla fine del § 6, ecc.). E su questi «snodi», per riprendere la metafora di p. 931 e ampliarne la portata, si tende a inserire quella gamma di «giustificazioni» e di «fondazioni» del numero che le diverse filosofie hanno via via elaborato. Dalle giustificazioni psicologistiche dei naturali al programma logicista di un Frege o di un Russell fino all'idea di chi oggi, rovesciando una tradizionale impostazione, vede nel continuo la nozione primaria, «la struttura soggiacente» in grado di «generare» le stesse «strutture discrete»

[Thom 1980, cap. IV]... In altri articoli della presente *Enciclopedia* (come «Continuo/discreto» e, per gli aspetti calcolistici e meccanici, ancora «Calcolo», «Automa» e «Analogico/digitale») sono esaminate queste tematiche articolate tra «applicazione» e «fondazione». Qui è sufficiente osservare, trasferendo un detto celebre di Mill, che la pluralità dei punti di vista, «è un bene e non un male». C'è piú di un architetto per la nostra città, ci sono piú vie per rispondere alla domanda «Cos'è un numero?» [G. G. e M. M.].

Bauer, H.
[1974] *Aspects of Modern Potential Theory*, in *Proceedings of the International Congress of Mathematicians, Vancouver B.C. 1974*, vol. I, Canadian Mathematical Congress, Montreal 1975, pp. 41-55.

Bell, E. T.
1937 *Men of Mathematics*, Simon and Schuster, New York (trad. it. Sansoni, Firenze 1966).

Bloor, D.
1976 *Knowledge and Social Imaginery*, Routledge and Kegan Paul, London.

Bombieri, E.
1976 *Hilbert's 8th Problem: an Analogue*, in Browder 1976, pp. 269-74.

Bourbaki, N.
1960 *Eléments d'histoire des mathématiques*, Hermann, Paris (trad. it. Feltrinelli, Milano 1963).

Browder, F.
1976 (a cura di) *Mathematical Developments Arising from Hilbert Problems*, American Mathematical Society, Providence R.I.

Chandrasekharan, K.
[1974] *The Work of Enrico Bombieri*, in *Proceedings of the International Congress of Mathematicians, Vancouver B.C. 1974*, vol. I, Canadian Mathematical Congress, Montreal 1975, pp. 3-10.

Courant, R.
1950 *Dirichlet's Principle, Conformal Mapping and Minimal Surfaces*, Interscience, New York - London.

Dickson, L. E.
[1919-23] *History of the Theory of Numbers*, 3 voll., Carnegie Institution of Washington, Washington; ed. Chelsea, New York 1952.

Dieudonné, J.
1977 *Panorama des mathématiques pures. Le choix bourbachique*, Gauthier-Villars, Paris.

Dieudonné, J., e altri
1978 *Abrégé d'histoire des mathématiques (1700-1900)*, Hermann, Paris.

Ellison, W. J., e Ellison, F.
1978 *Théorie des nombres*, in Dieudonné e altri 1978, vol. I, pp. 165-334.

Eulero, L.
[1751] *Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs*, in *Opera omnia*, Teubner und Orell-Füssli, Leipzig-Berlin-Zürich 1911-57, vol. II, pp. 240-53.

Gauss, C. F.
1801 *Disquisitiones arithmeticae*, Fleischer, Leipzig.

Grua, G.
1948 (a cura di) *Textes inédits de Leibniz*, Presses Universitaires de France, Paris.

Heath, Th. L.
1921 *A History of Greek Mathematics*, Clarendon Press, Oxford.

Hilbert, D.
1900 *Mathematische Probleme. Vortrag, gehalten auf dem Internationalen Mathematiker Kongress zu Paris 1900*, in «Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse», pp. 253-97 (trad. ingl. in Browder 1976, pp. 1-34).

Katz, N. M.
1976 *An Overview of Deligne's Proof of the Riemann Hypothesis for Varieties over Finite Fields (Hilbert's Problem 8)*, in Browder 1976, pp. 275-306.

Klein, J.
1934-36 *Die griechische Logistik und die Entstehung der Algebra*, in «Quellen und Studien zur Geschichte der Mathematik, Astronomie und Physik», sezione B, III, 1, pp. 18-105, e 2, pp. 122-235; ed. ingl. *Greek Mathematical Thought and the Origin of Algebra*, Mit Press, Cambridge Mass. 1968.

Kline, M.
1972 *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York.

Kuhn, Th. S.
1962 *The Structure of Scientific Revolutions*, University of Chicago Press, Chicago (trad. it. Einaudi, Torino 1976[3]).
1976 *Theory-change as structure-change*, in «Erkenntnis», n. 10, pp. 179-99.
1977 *The Essential Tension. Selected Studies in Scientific Tradition and Change*, University of Chicago Press, Chicago.

Lakatos, I.
[1961-74] *Proofs and Refutations. The Logic of Mathematical Discovery*, Cambridge University Press, London 1976 (trad. it. Feltrinelli, Milano 1979).

Leibniz, G. W.
[1702] *Specimen novum analyseos*, in *Mathematische Schriften*, vol. V, Schmidt, Halle 1858, pp. 350-61.

Montgomery, H. L.
1976 *Problems Concerning Prime Numbers (Hilbert's Problem 8)*, in Browder 1976, pp. 307-10.

Newton, I.
1707 *Arithmetica universalis; sive, De compositione et revolutione arithmetica liber*, Tooke, London.

Péter, R.
1957 *Játek a végtelennel. Matematikai kívülállóknak*, Bibliotheca, Budapest (trad. it. Feltrinelli, Milano 1973).

Richards, I.
1978 *Number Theory*, in L. A. Steen (a cura di), *Mathematics Today. Twelve Informal Essays*, Springer, Berlin - Heidelberg - New York, pp. 37-64.

Riemann, B.
1859 *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, in «Monatsberichte der Berliner Akademie», pp. 671-80.

Stevin, S.
1585 *L'Arithmetique de Simon Stevin de Bruges, contenant les computations des nombres arithmetiques ou vulgaires; aussi l'algebre, avec les equations de cinq quantitez*, Plantin, Leiden.

Thom, R.
1971 *Modèles mathématiques de la morphogenèse*, Accademia nazionale dei Lincei, Scuola normale superiore, Pisa.
1980 *Parabole e catastrofi*, Il Saggiatore, Milano.

Vallée, R.
1979 Intervento nella discussione di R. Thom, *Modélisation et scientificité*, in *Elaboration et justification des modèles (Applications en biologie)*, vol. I, Maloine, Paris, pp. 28-29.

Waismann, F.
1936 *Einführung in das mathematische Denken*, Gerold, Wien (trad. it. Boringhieri, Torino 1965).

Per tutta la **sua storia** l'**uomo** è stato affascinato dai numeri e pressoché ogni **civiltà** (cfr. anche **cultura/culture**) ha prodotto i suoi esperti di aritmetica, quella che Gauss chiamava «la regina delle matematiche»: prima che di matematici «puri» si è trattato di maghi e stregoni (**cfr. magia, stregoneria**), cabalisti (cfr. **cabala**), compilatori di calendari (cfr. **calendario**, ma anche **ciclo** e **periodizzazione**), astrologi (cfr. **astrologia**), preti (cfr. **religione**), creatori di miti e/o di filosofie (cfr. **mythos/logos, filosofia/filosofie**), tecnici esperti della **misura** dei terreni, cioè «geometri» nel senso originale del termine (cfr. però anche **geometria e topologia**). Il numero appare del resto una delle nozioni piú comuni e familiari della **mente** e, comunque, una componente fondamentale del **linguaggio** (cfr. anche **apprendimento**). Ma la sua articolazione nel contesto delle **matematiche** e la scoperta dei suoi nessi con altre nozioni di base rivela il ruolo sempre piú rilevante dell'astrazione (cfr. **astratto/concreto**). Gli stessi sviluppi della notazione (cfr. **segno, simbolo, scrittura**), l'introduzione dello **zero**, la creazione dei vari sistemi numerici – numeri interi, razionali, reali, complessi –, le questioni di fondo dell'**approssimazione** numerica, le estensioni piú o meno ardite (per esempio la costruzione dei «numeri transfiniti»: **cfr. infinito**), la cosiddetta aritmetizzazione dell'analisi e della geometria (cfr. **continuo/discreto**) e infine la stessa questione dei fondamenti dell'aritmetica (cfr. **insieme e logica**), si sono via via intrecciati con le esigenze del **calcolo** (cfr. anche **algoritmo**). Lo sviluppo di opportuni strumenti matematici (cfr. **curve e superfici, funzioni, applicazioni** e, piú in generale, **strutture matematiche**) ha d'altra parte consentito una vasta problematica interna alla matematica stessa, la teoria dei numeri (per aspetti specifici cfr. in particolare **divisibilità, razionale/algebrico/trascendente**). Se alcune delle «sfide» piú stimolanti per l'intelligenza dei ricercatori provengono proprio da questo settore, non va dimenticato il ruolo essenziale svolto dai numeri nella modellizzazione (**cfr. modello, teoria/modello**) del **reale**, nelle discipline piú svariate (cfr. **disciplina/discipline**), dalla **astronomia** e dalla **fisica** alle scienze del vivente (cfr. **gene, vita**) e alle stesse scienze sociali (cfr. **economia, società**). Gli sviluppi dei mezzi tecnici connessi al calcolo (cfr. **abaco, automa, analogico/digitale** e, per aspetti piú generali, **strumento, macchina** e **tecnica**) hanno permesso di sofisticare, talora in modo estremamente sottile, i procedimenti via via seguiti (cfr. **metodo**) per «dare numeri alle cose».

Zero

«IO Puoi descriverlo a parole? || LEI È tutto | è nulla | è la morte | la morte meccanica degli esseri umani | un buco nero | Zero».

[Laing 1976, trad. it. p. 32].

1. *Premessa. La «scatola vuota».*

La teoria matematica dei numeri naturali (1, 2, 3, 4, ecc.) si basa sul fatto che le operazioni fondamentali per tali numeri sono regolate da ben determinate «leggi». Un modello concreto che bene si presta a metterne in evidenza la base intuitiva può venir costruito come segue [cfr. Courant e Robbins 1941, trad. it. pp. 35 sgg.]. Invece di usare i soliti simboli 1, 2, 3, 4, ecc. si possono rappresentare i numeri che indicano gli oggetti di dati insiemi come insiemi di palline poste in apposite scatole rettangolari, una pallina per ciascun oggetto (cfr. fig. 1). È immediato, allora, interpretare le operazioni sui naturali: per esempio, per addizionare due numeri interi m e n si possono porre le scatole corrispondenti l'una accanto all'altra e si rimuove quindi la parete divisoria comune (cfr. fig. 1*a*); per moltiplicare m e n si forma una nuova scatola con m righe, ciascuna composta di n palline, ottenendo cosí anche n colonne, ciascuna composta di m palline. Le «leggi dell'aritmetica» vengono dunque a corrispondere a proprietà di queste scatole (cfr. figg. 1*b*, 1*c*).

Si può anche «leggermente estendere» [*ibid.*, p. 37] il dominio dei naturali rappresentati da scatole di palline introducendo un nuovo «numero», lo zero,

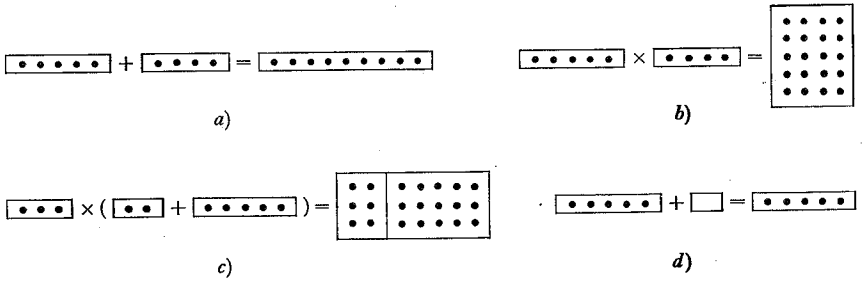


Figura 1.

Un modello «concreto», per molti versi analogo all'antico abaco, per l'interpretazione delle operazioni aritmetiche fondamentali (sull'insieme dei naturali) [Courant e Robbins 1941, trad. it. p. 36]. Esso consente un'agevole e intuitiva realizzazione di molte «leggi dell'aritmetica». In *a*) è interpretata l'addizione, in *b*) la moltiplicazione, *c*) offre un immediato riscontro della legge distributiva, e *d*) illustra infine una proprietà aritmetica dello zero, quella di essere elemento neutro per l'addizione (esempio: $5+0=5$).

rappresentato da *una scatola vuota*. È allora abbastanza facile ricavare le sue proprietà aritmetiche: se si indica la scatola vuota con l'usuale simbolo 0, si ha subito, per ogni naturale n, $n+0=n$, poiché $n+0$ indica l'addizione di una scatola n con la scatola vuota (cfr. fig. 1*d*). Per $n \cdot 0=0$ bisogna riflettere forse qualche istante di piú: tuttavia $n \times 0$ altro non è che una scatola senza colonne, e una scatola *senza colonne* è appunto una scatola *vuota*...

Proprio una rappresentazione «concreta» dei numeri (naturali) e delle operazioni fondamentali cosí «rudimentale» mostra come nella «leggera estensione» non ci sia apparentemente alcuna difficoltà, alcun mistero. Eppure intere culture, dotate talora di una matematica progredita e sofisticata, non sono state in grado di, o hanno esitato a, compierla; altrove la comparsa dello zero ha costituito l'intrusione di un vero e proprio «sovversivo» dalla Legge & ordine matematici... Col senno di poi, tutto sembra ridursi a un'agile combinatoria... Secondo un celebre aneddoto, però, uno dei piú sottili indagatori del concetto di numero, Richard Dedekind, immaginava gl'insiemi semplicemente come dei sacchi contenenti determinati oggetti, mentre il creatore della teoria degli insiemi, Georg Cantor, quando diede a conoscere la sua rappresentazione di un insieme, «drizzò la sua colossale figura, descrisse con il braccio alzato un gesto grandioso e disse con uno sguardo sperduto nel vuoto: "Io immagino un insieme come un abisso"» [cfr. Meschkowski 1960, trad. it. pp. 62-63]. Segno *di qualcosa* e, allo stesso tempo, «segno di niente», dunque «detestabile figura» [cfr. Badiou 1969, p. 164], lo zero ha, in particolare, il suo proprio «abisso». Per gettarvi almeno uno sguardo, sarà opportuno tornare indietro nel tempo, a molto prima della vittoria della concezione attuale di che cosa «sono» i numeri, a molto prima anche dello scambio di battute tra Dedekind e Cantor, a prima ancora della stessa affermazione e diffusione dello zero – come concetto e come simbolo – nella matematica dell'Occidente.

2. *Il nulla e Fredegiso.*

C'era una volta, nei secoli «bui» del medioevo, l'abate Fredegiso di Tours (morto appunto nell'834), la cui fama è legata principalmente a una *Epistola de nihilo et tenebris* [in Migne, *Patrologia latina*, CV, coll. 751-56], in cui, detto in breve, da una interpretazione letterale del *Genesi*, là ove si afferma che Dio ha creato il mondo dal nulla (*ex nihilo*), si conclude che il nulla è qualcosa di reale. Ora, qualcuno, come De Wulf nella sua *Histoire de la philosophie médiévale* (1925), liquida gli argomenti di Fredegiso come semplici *enfantillages* o *sophismes verbaux*. Altri storici del pensiero medievale sono piú clementi e li valutano come qualcosa di piú che «un puro esercizio di abilità dialettica» [cfr. per esempio Vasoli 1961, p. 53]. Comunque pare «piú facile sorridere della soluzione di Fredegiso, che non trovarne un'altra di maggior consistenza» [Geymonat 1952, ed. 1953 p. 103].

Infatti: Fredegiso si pone la domanda «nihilne aliquid sit, an non», se cioè il nulla (*nihil*) sia qualcosa (*aliquid*) oppure no. Ora, «si quis responderit

"Videtur mihi nihil esse", ipsa ejus quam putat negatio compellit eum fateri aliquid esse nihil, dum dicit "Videtur mihi nihil esse". Quod tale est quasi dicat "Videtur mihi nihil quiddam esse"» [*Epistola de nihilo et tenebris*, in Migne, *Patrologia latina*, CV, col. 751]. Il latino barbaro e scolastico di Fredegiso è quasi trasparente: perché si possa predicare qualcosa di un soggetto, questo soggetto deve essere qualcosa di determinato. Poiché «tutti siamo convinti di poter parlare sensatamente del "nulla", di intenderci fra noi allorché usiamo questo termine... esso deve avere per noi un significato ben determinato: "nihil aliquid significat". Proprio questo fatto però, che esso significhi qualcosa, che denoti un'effettiva realtà, sembra particolarmente ripugnante al pensiero comune» [Geymonat 1952, ed. 1953 p. 102]. Il «coraggio» di Fredegiso sta nel concludere *l'esistenza del nulla* sfidando tale «ripugnanza» e sancendo questo scandalo dell'ontologia e della logica. Certo, come osserva Gilson [1944, trad. it. p. 236 in particolare], si rivelerebbe qui una concezione della logica e del linguaggio integralmente realistica. L'interesse maggiore risiede però nel fatto che tale realismo si manifesta proprio in riferimento a una specifica idea, appunto quella del *nulla*. Sia lecito un accostamento. Hegel, *Scienza della logica* [1812-16]: «Quando la metafisica posteriore, soprattutto la cristiana, rigettò la proposizione che dal nulla venisse nulla, essa affermò un passaggio dal nulla nell'essere. Per quanto, ora, questa proposizione fosse da lei presa sinteticamente o in guisa semplicemente rappresentativa, pur nondimeno anche nella piú imperfetta unione è contenuto un punto in cui l'essere e il nulla coincidono, e la differenza loro sparisce... Cosí perfino in Dio la qualità, cioè l'attività, la creazione, la potenza ecc., contiene essenzialmente la determinazione del negativo; coteste qualità consistono nella produzione di un altro» (trad. it. I, pp. 72, 73).

3. *Zero: mancanza di segno o segno di una mancanza?*

Che la contrapposizione tra o e le altre cifre significative (in particolare: tra o e 1 nella notazione binaria) adombrasse «il passaggio del nulla all'essere» era già opinione di Leibniz (cfr. l'articolo «Calcolo» in questa stessa *Enciclopedia*, in particolare alla p. 396). Qui si vuol sostenere che le ambiguità del «nulla», che il realismo estremo di Fredegiso dissipava sfidando il senso comune, si ripropongono nel caso dello o entro la tradizione matematica dell'Occidente. Si potrebbe addirittura sostenere che la problematica concernente la giustificazione dello zero entro le matematiche non è altro che una particolare versione del problema del nulla di Fredegiso [cfr. Geymonat 1952, ed. 1953 pp. 105 sgg.].

«Ma che tipo di folle simbolo è mai questo [cioè o], che per l'appunto, significa il nulla? È una cifra, o non lo è? 1, 2, 3, 4, 5, 6, 7, 8 e 9 stanno tutti per numeri che si possono intuire o comprendere, ma o? Se o è nulla, allora dovrebbe essere sempre nulla. Ma qualche volta è nulla e qualche altra volta è qualcosa: $3+0=3$ e $3-0=3$, qui zero è nulla, nel risultato non compare più.

anche quando viene collocato prima di un numero, non lo cambia, scrivere 03 è come scrivere 3, e anche qui lo zero è nulla, *nulla figura!* Ma se si scrive lo zero *dopo* un numero, esso moltiplica allora improvvisamente il numero per dieci: $30=3\times 10$. Cosí, ora, zero è qualcosa, qualcosa di incomprensibile ma potente, se pochi 'nulla' possono mutare un piccolo numero in uno grandissimo» [Menninger 1957, trad. ingl. p. 422].

Ancora nel XV secolo, a piú di duecento anni da quando Leonardo Pisano (Fibonacci) nel suo *Liber Abaci* (1202) aveva annunziato che con le «novem figure Indorum» e con «hoc signum o, quod arabice chepirum appellatur» si scriveva in linea di principio *qualsiasi* numero, un autore francese definiva lo zero «une chiffre donnant umbre et encombre», un segno che produce confusione e difficoltà: altri, nel constatare che ogni aggiunzione di o dopo un numero appunto lo moltiplica per dieci, riscontrava con meraviglia che esso «ommia ex nichillo creat, conservat atque gubernat» [citati *ibid.*, pp. 422, 423]. Carico talora di pregnanza entro la «metafisica cristiana», visto ora quasi come un demone, ora quasi come un dio, lo zero, entro il contesto dell'arte del calcolo, realizzava appunto la violazione del *ex nihilo nihil fit*, la proposizione in cui, alternativamente, si può scorgere o «la vana tautologia che nulla è nulla» o l'esclusione di «alcun effettivo divenire» [Hegel 1812-16, trad. it. I, p. 72].

Ma da dove veniva questo «sovversivo»? La risposta non è facile, il suo cammino è tutt'altro che pacifico e lineare. Nelle pagine immediatamente seguenti si delineeranno allora alcuni momenti di questo cammino, senza pretesa alcuna di completezza, ma con maggior sensibilità per quelli in cui maggiormente si dispiegano *umbre et encombre*, cioè le difficoltà concettuali che all'uso e alla definizione dello zero si sono via via legate, a causa del suo, come si è detto, statuto ambiguo: *segno di una mancanza o mancanza di segno?* [cfr. del resto le osservazioni di Badiou 1969].

3.1. La «lacuna» babilonese.

L'importanza di una *notazione posizionale* per il calcolo è stata sottolineata altrove in questa stessa *Enciclopedia* (cfr. in particolare il citato articolo «Calcolo» alle pp. 382-84). È altresí noto che il sistema sessagesimale escogitato

a) *b)*

Figura 2.

La «mancanza del segno» (*a*) e «il segno della mancanza» (*b*) nella notazione babilonese. Nel periodo antico un segno come quello riprodotto in *a*) può significare tanto $2\times 60+2$ quanto $20\times 60^2+2$, cioè tanto 122 quanto 7202: l'ambiguità veniva usualmente chiarita dal contesto. Nel periodo seleucidico, invece, due piccoli cunei disposti obliquamente funzionano da indicatore della mancanza di una cifra. Cosí in *b*) il nostro $7202=$ $=2\times 60^2+0\times 60+2$ è scritto in modo non ambiguo ed è facilmente distinguibile da ⟡⟡ ⟡⟡, cioè da $2\times 60+2$ [Boyer 1968, trad. it. p. 32].

dai Babilonesi «costituisce la prima comparsa del fondamentale "principio della posizione" nella scrittura dei numeri» [Cajori 1928, p. 4], ma con una singolare lacuna: «Nella sua applicazione generale e sistematica, questo principio infatti esige un simbolo per lo zero» [*ibid.*], ma questo manca nelle tavolette che risalgono ai primi secoli del II millennio a. C. (periodo babilonese antico) anche se talvolta viene lasciato uno *spazio vuoto* là dove si collocherebbe uno zero. Un accorgimento non privo di difficoltà (cfr. fig. 2*a*), anche se in molti casi era di fatto possibile eliminare l'ambiguità grazie al contesto; comunque «la mancanza di un simbolo per lo zero, come quello che oggi ci permette di distinguere a prima vista tra 22 e 202, deve avere costituito un grave inconveniente» [Boyer 1968, trad. it. p. 32]. Inconveniente aggirato però nelle tavolette degli ultimi secoli del I millennio a. C. (periodo seleucidico, o forse anche prima? [cfr. Ifrah 1981, p. 402 nota]): un segno apposito, consistente di due piccoli cunei disposti obliquamente, funziona da indicatore dello spazio in cui manca una cifra (cfr. fig. 2*b*). Tuttavia tale indicatore è impiegato dai matematici soprattutto per «vuoti» intermedi. Per qualche storico delle matematiche ciò sarebbe spia del fatto che «i babilonesi dell'antichità non giunsero mai a un sistema le cui cifre avessero un valore posizionale assoluto» [Boyer 1968, trad. it. p. 32; cfr. però le osservazioni di Ifrah 1981, pp. 400-2]. Comunque le vicissitudini della notazione babilonese bene esemplificano l'oscillazione di cui sopra: mancanza di segno / segno di una mancanza.

3.2. «L'occhio» dei Maya.

Per «la prima applicazione compiuta e sistematica del simbolo per lo zero e del principio di posizione» [Cajori 1928, p. 4] si deve lasciare il vecchio continente e spostarsi tra i Maya dello Yucatán in un'epoca che corrisponde circa agl'inizi dell'era cristiana. Il sistema maya, com'è noto, sembra strettamente legato al calendario. Al primo ordine, l'unità rappresenta 1 giorno (*kin*) e 20 giorni costituiscono 1 «mese» (*uinal*) cioè l'unità dell'ordine immediatamente superiore; 18 mesi costituiscono l'unità del terzo ordine o «anno» (*tun*, cioè 360 giorni; per ottenere l'anno solare i Maya aggiungevano nel calendario cinque giorni: $18 \times 20 + 5 = 365$), 20 anni costituiscono un'unità del quarto ordine

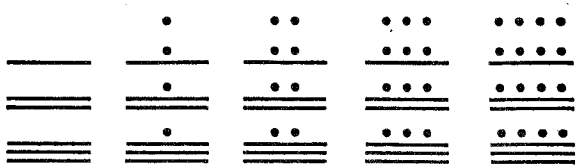


Figura 3.

I simboli maya per i numeri da 1 a 19 (procedendo da sinistra verso destra). Si è lasciato appositamente il «posto vuoto» per lo zero (ma si veda la successiva figura 5). Questi simboli, nelle rappresentazioni sacre e ufficiali, venivano combinati con le celebri *teste* che denotavano i vari ordini (come viene esemplificato nella figura 4) [cfr. Smith 1925, ed. 1958 p. 44].

(*katun*, cioè 7200 giorni), 20 di queste unità fanno un'unità del quinto ordine (*baktun* 'ciclo', cioè 144 000 giorni), ecc. Nelle rappresentazioni ufficiali e sacre delle teste raffigurano i vari ordini, ma le unità di ogni ordine vengono «contate» mediante un'elegante combinazione di punti e linee secondo la convenzione seguente: 1, 2, 3 e 4 vengono rappresentati da uno, due, tre, quattro punti rispettivamente; una linea raggruppa cinque unità (cfr. fig. 3). In questa notazione il valore attribuito ai segni dipende dunque dal posto che il segno occupa, ma ogni particolare ordine ha il suo «nome», rappresentato dalla testa che viene affiancata al numerale (cfr. fig. 4). In questo contesto, lo zero non è ancora necessario. Ma nei manoscritti maya i 19 simboli costruiti con punti e linee che rappresentano i numeri da 1 a 19 perdono via via il loro legame con la notazione ufficiale e sacerdotale esemplificata nella figura 4 per dare luogo a una vera e propria notazione posizionale astratta in cui compare un simbolo per lo zero, una sorta di occhio semichiuso, come appare nella figura 5. Una paziente ricerca storica [cfr. per esempio Menninger 1957, trad. ingl. pp. 62, 404] ha permesso di ricostruire, per lo meno parzialmente, questo sottile trapasso (in cui il legame con il calendario resta evidenziato, comunque, dal fatto che l'unità del terzo ordine resta sempre costituita da diciotto unità del secondo ordine; cfr. anche la didascalia della figura 5) ma «siamo di fronte sempre a un enigma nella storia della cultura: una notazione posizionale astratta, *provvista di zero*, basata sul 20, che compare in apparente isolamento lontano nel Nuovo Mondo» [*ibid.*, pp. 404-5].

3.3. Lo οὐδέν di Tolomeo.

Quasi nulla si sa della notazione impiegata dai primi matematici greci (per esempio, dai pitagorici), mentre sono noti pregi e limiti del sistema «letterale» sviluppato successivamente nella cultura greca (cfr. quanto osservato nell'articolo «Modello» in questa stessa *Enciclopedia*, IX, pp. 389-91 [per una dettagliata discussione delle diverse varianti cfr. per esempio Heath 1931, ed. 1963 in particolare pp. 14-20; cfr. anche Ifrah 1981, pp. 277-90]). Papiri riportabili alla prima parte del periodo alessandrino (gli ultimi tre secoli avanti Cristo) contengono qualcosa di simile a un simbolo che «proprio come lo zero babilonese del periodo seleucidico, veniva impiegato per indicare cifre mancanti» [Kline 1972, p. 132].

La testimonianza piú interessante è forse quella offerta dai manoscritti bizantini dell'opera di Claudio Tolomeo. Il sistema sessagesimale di origine babilonese si era rilevato particolarmente utile nei calcoli astronomici e nell'opera di Tolomeo è pienamente articolato un sistema di frazioni sessagesimale che permette una notevole precisione [cfr. ancora Heath 1931, ed. 1963 pp. 23-24]: la circonferenza di un cerchio è divisa in 360 τμήματα o μοῖραι (letteralmente 'segmenti' o 'parti': oggi si direbbe gradi) e ogni parte viene divisa in 60 «minuti» (o «primi sessantesimi»), ciascuno dei quali è a sua volta diviso in 60 «secondi sessantesimi» e, in linea di principio, questo procedimento può venire iterato *ad libitum*. Quando non c'è qualche particolare denominazione

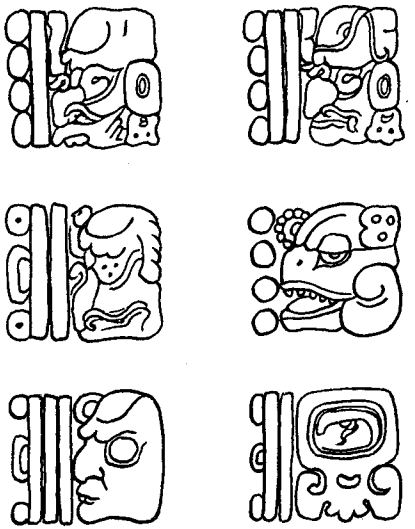


Figura 4.

La notazione «ufficiale» maya. Dalla riga piú alta e procedendo da sinistra a destra: 9 unità del quinto ordine, cioè $9 \times (20^3 \times 18) = 1\,296\,000$; 14 unità del quarto ordine, cioè $14 \times (20^2 \times 18) = 100\,800$; 12 unità del terzo ordine, cioè $12 \times 360 = 4320$; 4 unità del secondo ordine, cioè $4 \times 20 = 80$; 17 unità del primo ordine, cioè $17 \times 1 = 17$ [Menninger 1957, trad. ingl. p. 404]. Si osservi che, se non vi fosse al terzo ordine l'anomalia per cui 18 «mesi» costituiscono un «anno» – che è spia dello stretto legame con il calendario – la faccia che rappresenta l'ordine n ($n = 1, 2, 3, 4$, ecc.) verrebbe a denotare la potenza $n - 1$ di 20 (a cominciare da 20^0, cioè 1).

Notazione maya					
Trascrizione in cifre decimali	1 0	1 17	15·20 0	360 0 0	19·360 13·20 13
Valori	20	37	300	360	7113

Figura 5.

Ai diciannove segni della figura 3 si è aggiunto anche un simbolo per lo zero. In questa notazione posizionale i Maya scrivono i numeri verticalmente [per le origini e i possibili impieghi di questa notazione, cfr. ad esempio Smith 1925, ed. 1958 pp. 44, 45]. Si osservi infine che non trattandosi di una notazione vigesimale in senso stretto (cfr. quanto osservato nella figura 4), lo zero maya (al contrario del nostro!) non svolge appieno il ruolo di operatore aritmetico. Come si vede nella figura, 100 maya corrisponde al nostro 360 e non a 400, come sarebbe in un sistema vigesimale in senso stretto. (D'altra parte il nostro 400 si scrive nella notazione maya 120, poiché $400 = 1 \times 360 + 2 \times 20 + 0$). Se ne deve concludere «la non-identità della funzione svolta dallo zero maya con quella svolta dal nostro zero» [Ifrah 1981, p. 451 nota].

delle frazioni cosí ottenute, viene introdotto il simbolo o che abbrevia οὐδὲν ἑξηκοστόν (letteralmente 'nessun sessantesimo') e simili. In questo contesto il simbolo può comparire anche in posizione terminale (nel senso che, per esempio, ci si imbatte in scritture come μοιρῶν o α′ β″ o‴ che oggi si scriverebbero $0^0\ 1'\ 2''\ 0'''$).

La presenza di un simbolo o in Tolomeo (e congetturalmente in autori precedenti [cfr. Smith 1925, ed. 1958 p. 69, nota 4] difficilmente poteva venir non enfatizzata. Alexander von Humboldt: «Un vero e proprio simbolo zero, che sta per l'assenza di una qualche unità, viene utilizzato da Tolomeo nella sua scala sessagesimale discendente quando mancano gradi, minuti o secondi... Lo zero è dunque molto piú vecchio, nell'Occidente, dell'invasione degli Arabi e dell'opera di Massimo Planude dedicata agli ἀριθμοὶ ἰνδικοί» [1829, p. 224; cfr. anche le osservazioni di Cajori 1928, p. 54]. Un'autorevole tradizione vuole inoltre che il simbolo o attualmente in uso altro non sia che una modificazione dell'o dell'οὐδέν di Tolomeo. Si può però obiettare che «sebbene il simbolo indicante una posizione vuota che compare in alcune delle versioni esistenti delle tavole delle corde di Tolomeo sembri simile a un omicron, i piú antichi simboli per lo zero che compaiono nelle frazioni sessagesimali greche sono forme rotonde variamente decorate e nettamente diverse dalla forma di un semplice uovo. Inoltre, quando nel XV secolo dell'Impero bizantino venne elaborato un sistema posizionale decimale a partire dalle antiche cifre alfabetiche lasciando cadere le ultime diciotto lettere e aggiungendo alle prime nove lettere un simbolo per lo zero, il segno indicante lo zero assunse forme molto diverse da quella di un omicron. Talvolta assomigliava a una forma rovesciata della nostra lettera minuscola h, talaltra compariva come un punto» [Boyer 1968, trad. it. pp. 251-52; cfr. anche Neugebauer 1957, cap. I, § 10]. Forse una congettura intermedia è possibile [cfr. per esempio Waerden 1961, pp. 56-68; e Boyer 1968, trad. it. p. 250]: il penetrare della cultura matematica alessandrina verso Oriente, in Persia e poi nell'India, avrebbe posto le premesse dell'«invenzione» dello zero nella cultura indiana: come ogni grande innovazione concettuale, anche lo zero sarebbe rimasto un *freak*, cioè una stranezza, una stravaganza, una semplice devianza se non avesse trovato una opportuna «nicchia» ove collocarsi. E la formazione di «nicchie» del genere richiede talora lavori di secoli e incroci di piú tradizioni.

3.4. Il *śūnya* indiano.

Il sistema di numerazione decimale di cui oggi si fa ancora larghissimo uso (cfr. però le osservazioni nel citato articolo «Calcolo», II, pp. 383-84 e 395-96) è noto come sistema «indo-arabico». Esso «deriva semplicemente da una nuova combinazione di tre principi fondamentali, tutti di origine molto piú antica: 1) una base decimale; 2) una notazione posizionale; 3) un simbolo diverso per ciascuna delle dieci cifre» [*ibid.*, p. 251]. Ora, anche se nessuno di questi principî venne originariamente inventato dagli Indiani, è indubbio che l'elaborazione di questo sistema rappresenti uno dei piú rilevanti contributi della cultu-

ra dell'India alla crescita della matematica, anche se la comprensione della portata di tali innovazioni deve essere stata agl'inizi ben limitata (il che rivaluta il ruolo dei matematici arabi di cui al paragrafo successivo, come qualcosa di piú che semplice tramite per il passaggio delle cifre indiane da Oriente a Occidente [cfr. le osservazioni di Kline 1980, p. 111]). L'originalità della matematica indiana sta invece nell'aver «per la prima volta collegato i tre principi a formare il sistema di numerazione moderno» [Boyer 1968, trad. it. p. 251], anche se «la nostra perfezionata notazione indo-arabica venne prodotta attraverso una lenta evoluzione» [Cajori 1928, p. 54].

Già su un piatto del 595 d. C. è scritta la data, 346, in notazione posizionale decimale [cfr. Struik 1967, p. 71; cfr. anche Boyer 1968, trad. it. p. 280], ma «la comparsa certa di un simbolo per zero in India si trova per la prima volta in una iscrizione dell'876 a Gwalior, in cui 50 e 270 appaiono entrambi scritti con uno zero» [Smith 1925, ed. 1958 p. 69; cfr. fig. 6]. Ora, «senza lo zero il sistema di numerazione indiano non sarebbe stato certo meglio di molti altri, dato che la sua peculiarità piú distintiva è proprio il valore locale» [*ibid.*]; ma, in questo come in altri casi, per usare le stesse parole che Ifrah usa per lo «zero» babilonese, occorre sempre «distinguere tra la "data" presunta di una "invenzione", quella della sua diffusione e quella delle prime testimonianze» [1981, p. 402 nota]. La questione è delicata: una corrente storiografica sembra insistere sul fatto che gli Indiani non avrebbero posseduto un simbolo per lo zero ***prima*** del IX secolo; altri invece sposta l'impiego di una notazione decimale scritta provvista di zero anche prima di Sebokt, sulla base di iscrizioni del Sud-Est asiatico [cfr. per esempio *ibid.*, pp. 466 sgg.].

Comunque, a prescindere dall'enigma maya – ove peraltro la stessa notazione posizionale in base 20 e provvista dello zero sembra utilizzata meramente per esprimere il tempo trascorso tra due date significative, piú che per essere utilizzata in veri e propri calcoli [cfr. Smith 1925, ed. 1958 p. 44; cfr. anche quanto detto sopra, § 3.2] –, sia che venga anticipato dalla notazione greca (cfr. § 3.3) o che derivi dal circolo poi usato nei caratteri «letterali» brāhmī per il 10, o ancora da un punto utilizzato dagli Indiani, magari racchiuso da un circoletto per meglio evidenziarlo, non ci sono molte probabilità che l'origine del simbolo 0 – come del resto dei simboli delle altre nove cifre decimali venga chiarita al di là di ogni ragionevole dubbio... Quel che interessa qui è però lo slittamento da semplice indicatore di un posto vuoto, come del resto mostra ancora uno dei termini del sanscrito, *śūnya* (che in origine significa appunto 'vuoto'; altri termini sono: *kha* 'cielo', *gagana* 'spazio', *ambara* 'atmosfera', ***bindu*** 'punto', ecc. [cfr. Ifrah 1981, pp. 472-73, 486]), a numero come

Figura 6.
Dall'iscrizione di Gwalior [Ifrah 1981, p. 463].

gli altri, assoggettato a regole di calcolo che estendono «in modo naturale» le regole del calcolo (cfr. le osservazioni informali del § 1). Ma quanto «naturale»? Come si è visto per altre estensioni delle «leggi dell'aritmetica» fuori dell'abituale dominio dei naturali 1, 2, 3, 4, ecc., è in gioco anche qui un equilibrio assai delicato, tra intuizione e convenzione, tra economia di pensiero e intelligibilità degli enti matematici introdotti.

Ora, nel caso specifico dello zero, proprio l'atteggiamento dei matematici indiani è doppiamente significativo: e sotto il profilo del perfezionamento delle tecniche del calcolo e sotto quello del divorzio dal senso comune a cominciare dal profondo rivolgimento intellettuale che la notazione con lo zero impose rispetto alle rappresentazioni sull'abaco (cfr. fig. 7).

Qualche esempio. Il matematico e astronomo Brahmagupta nel suo *Brahma Sphuṭa Siddhānta* (628 d. C.) discute sei operazioni (addizione, sottrazione, moltiplicazione, divisione, potenza, estrazione di radice) su «crediti», «debiti» e «nulla» (*dhana*, *ṛṇa*, *kham*), cioè su numeri positivi, numeri negativi e sul *numero* zero [*ibid.*, p. 487 nota]. Quindi lo zero, concepito in precedenza come operatore aritmetico (cioè come un segno che aggiunto a una cifra «significativa» la moltiplica per dieci), comincia ad essere trattato come un ente matematico a sé. Nella prospettiva del presente articolo, allora, piú che chiedersi quale sia l'origine del segno, la sua provenienza, ecc. parrebbe interessante chiedersi «a partire da che epoca e in che modo, questo concetto (che, all'origine, denotava il vuoto, la *colonna vuota* dell'abaco) si è arricchito acquistando il senso di "nulla", di 10 – 10» [*ibid.*]. Tanto piú che questo creativo slittamento di significato si è poi riprodotto (come il lettore avrà modo di vedere nei paragrafi successivi) nella matematica dell'Occidente. Ma «sfortunatamente, allo stato attuale delle nostre conoscenze, è impossibile rispondere a un quesito del genere» [*ibid.*].

Inoltre: il matematico indiano Mahāvīra, del IX secolo d. C., cosí enuncia

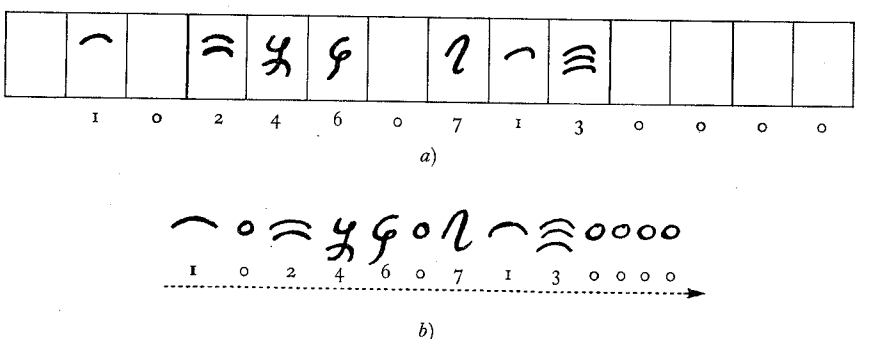


Figura 7.
Evoluzione dello zero: da «posto vuoto» sull'abaco a cifra scritta. Lo stesso numero 1 024 607 130 000 simbolizzato in *a*) sull'abaco a colonne e in *b*) con nove cifre indiane compreso il circoletto per lo zero [Ifrah 1981, p. 486].

le regole del calcolo delle quattro operazioni fondamentali nel caso dello zero: «Un numero moltiplicato per zero, dà zero, e tale numero resta immutato quando viene *diviso*, aumentato o diminuito di zero» [citato e discusso in Smith 1923, ed. 1958 p. 162]. Come dire, per ogni naturale $n \geq 1$,

(1) $n \times 0 = 0$

(2) $n : 0 = n$

(3) $n + 0 = n$

(4) $n - 0 = n$

Ora se si considera *zero* come equivalente a *nulla*, *nessuno*, convenzioni come la (3) e la (4) appaiono abbastanza plausibili. Ma qualcuno potrebbe già sospettare convenzioni come la (1) [Black 1977, p. 770; cfr. però le osservazioni al § 1].

Infine qualche giustificazione intuitiva potrebbe venir escogitata anche per la (2): se si possiede, ad esempio, una torta, e non c'è *nessuno* per dividerla, si resta con l'intera torta. Ma di fronte alle difficoltà che immediatamente scaturiscono da una convenzione del genere (vi si ritornerà piú avanti) non è «ragionevole» [*ibid.*] *vietare la divisione per zero*, come del resto è oggi insegnato in ogni manuale (cfr. oltre)?

Si deve, però, concluderne che Mahāvīra peccava di irragionevolezza? E che di una diversa irragionevolezza si rendeva colpevole anche l'indiano Bhāskara (nato circa verso il 1114) quando, oltre a riprendere le convenzioni (1), (3) e (4), a proposito della divisione per zero si impegnava audacemente in un trapasso dal finito all'infinito che doveva giustificare *teologicamente*? Bhāskara scriveva infatti: «Enunciato: Dividendo 3, Divisore 0. Quoziente la frazione 3/0. Questa frazione, il cui denominatore è zero, viene definita una quantità infinita. In questa quantità, consistente in ciò che ha come divisore lo zero, non v'è nessuna alterazione, anche se vi viene aggiunto o tolto molto: infatti nessun mutamento ha luogo nella infinità e immutabilità di Dio» [citato e discusso in Boyer 1968, trad. it. p. 259; cfr. anche Smith 1923, ed. 1958 pp. 277-78]. Boyer commenta: «Questa affermazione suona promettente, ma l'ulteriore asserzione di Bhāskara che $(a/0) \cdot 0 = a$ mostra la mancanza di una chiara comprensione del problema» [1968, trad. it. p. 259]. Questi atti «irragionevoli», questa «mancanza di comprensione», sono però germi da cui può dispiegarsi una rilevante crescita matematica, appena questa si situi nel contesto opportuno (si tornerà piú avanti sulla questione, alle pp. 1340-41).

3.5. La mediazione araba.

Nella cultura dell'Occidente la prima menzione della notazione indiana si ha nel 662 d. C. quando il vescovo siriano Severo Sebokt polemicamente contrappone alla cultura «ufficiale» di lingua greca tradizioni scientifiche differenti, tra cui menziona, degli Indiani, «le sottili scoperte astronomiche, piú ingegnose di quelle dei Babilonesi e dei Greci», nonché «i loro preziosi metodi di calcolo, che superano ogni descrizione». E aggiunge: «Voglio solo dire che qui i calcoli vengono effettuati per mezzo di nove segni» [citato e discusso in Smith 1923, ed. 1958 pp. 166-67; cfr. anche 1925, ed. 1958 p. 72]. Il riferimento a *nove* invece che a *dieci* simboli mostra però che lo zero non è qui preso in considerazione. La tradizione vuole che sia nel 733 che un insieme di tavole astronomiche venga tradotto, per ordine del califfo di Baghdād, dal sanscrito all'arabo: e qui si troverebbe la prima precisa informazione circa la notazione indiana, zero incluso [cfr. *ibid.*]. Meno di un secolo piú tardi se ne doveva già avere buona conoscenza: verso l'825 il grande al-Khuwārizmī, il «philosopho Algo» della tradizione occidentale, compila un breve trattato inteso a spiegarne l'uso. È il testo che verrà tradotto in latino, probabilmente da Adelardo di Bath, verso il 1120, come *Liber Algorithmi de numero Indorum*.

Ricostruire come la notazione indiana abbia soppiantato nel mondo arabo un tipo di notazione alfabetica ricalcata su quella greca (ma ovviamente con lettere dell'alfabeto arabo) e come via via se ne siano prodotte differenti versioni non è compito facile. Numerose varianti erano emerse già in India; ma quelle presenti nella vasta area che va dalla Persia alla Spagna, unificata con le armi nel nome di Allah, sono cosí notevoli da far avanzare l'ipotesi di origini diverse per le forme «arabo-orientali» e per quelle «arabo-occidentali»: le prime proverrebbero piú direttamente dall'India, anche se con qualche non lieve modificazione, mentre le seconde sarebbero corruzioni di forme greche o romane. Ma non si entrerà qui nella questione [per una disamina del problema, cfr. per esempio Menninger 1957, trad. ingl. pp. 408-17; Ifrah 1981, pp. 501-3]: nella tematica del presente articolo, «sono i principi all'interno del sistema di numerazione che sono importanti, e non le forme specifiche che possono assumere le cifre» [Boyer 1968, trad. it. p. 277].

3.6. Della «cecità» di Gerberto d'Aurillac.

La denominazione 'indo-arabiche' per le nostre usuali cifre è dunque pienamente giustificata. Ma l'acquisizione di quei dieci simboli a noi cosí familiari ha notevolmente stentato a penetrare nella Cristianità. Il caso di Gerberto d'Aurillac (nel 999 papa Silvestro II) è abbastanza significativo: fu probabilmente il primo a insegnare in Europa l'uso delle cifre indo-arabiche ma... è per noi molto difficile valutare la portata di tale insegnamento. Intanto quasi nulla si sa delle sue fonti. Una ipotesi, ma difficilmente comprovabile, è che Gerberto, durante un viaggio in Spagna, sia venuto in contatto, probabilmente a Barcellona, con la cultura matematica moresca che cominciava a filtrare nella Cristianità (cfr. fig. 8), in particolare con le cifre di forma occidentale o *gobar* (letteralmente 'polvere'). Va altresí ricordato che in certi manoscritti contenenti le opere di Boezio compaiono cifre di forma abbastanza simile (i cosiddetti «apici»: cfr. fig. 9), impiegate usualmente come contrassegni per far di conto coll'abaco e si potrebbe pensare che da questi invece Gerberto venne a conoscenza del nuovo sistema. Infine, non si può escludere che gli apici boeziani siano una interpolazione posteriore [cfr. Smith 1925, ed. 1958 pp. 73-74; Boyer 1968, trad. it. p. 292].

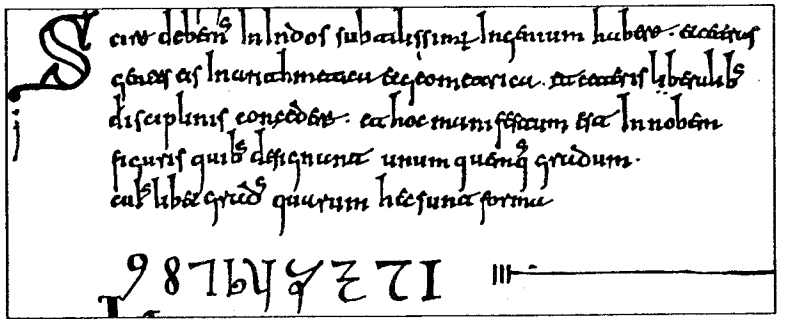


Figura 8.

Il primo manoscritto conosciuto (Biblioteca San Lorenzo del Escorial, Codex Vigilanus Ms. lat. d. 1.2, fol. 9v) in cui gli Europei riportano le nove cifre «significative» indo-arabiche. Si tratta di un manoscritto spagnolo (976 d. C.) in cui le cifre sono assai simili a quelle *gobar*. Manca un simbolo per zero [Ifrah 1981, p. 504].

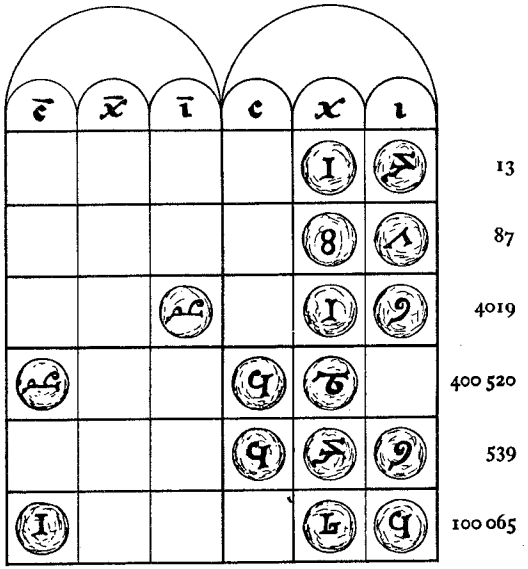


Figura 9.

La rappresentazione dei numeri naturali medianti *apici* sull'abaco perfezionato da Gerberto di Aurillac e dai suoi discepoli [Ifrah 1981, p. 507]. Su questo abaco, dotato di ventisette colonne raggruppate a tre a tre, gli apici prendevano un valore posizionale che variava a seconda della colonna in cui erano collocati. L'assenza di unità di un certo ordine era qui indicata semplicemente lasciando vuota la colonna corrispondente. In questo modo Gerberto era dispensato da «capire» e «introdurre» lo zero. La terminologia di Gerberto per i numeri da 1 a 9 era: *igin, andras, ormis, arbas, quimas, caltis, zenis, temenias, celentis* [per l'origine, assai oscura, di questa nomenclatura e il gioco delle varie influenze linguistiche – arabo, sanscrito, greco e latino – cfr. Menninger 1957, trad. ingl. p. 325]. Si aggiunse quindi successivamente anche lo zero, chiamato in questo contesto *sipos*, che pare corruzione del greco ψῆφος, letteralmente 'ciottolo' o 'pietruzza', termine destinato, come l'analogo latino *calculus*, a indicare poi 'conto', 'computo' e 'calcolo' (in quanto un sassolino denota l'ordine delle decine, due sassolini quello delle centinaia, ecc.).

Tra le cifre *gobar* (rappresentate nella figura 10) non compare lo zero: di fatto esso è inutile, perché dei «punti» collocati sulle cifre usualmente indicano «l'ordine» nel sistema *gobar*. Un punto per le decine, due punti per le centinaia, tre per le migliaia, ecc. Il sistema *gobar* utilizza dunque dei «nomi» in modo analogo al primo sistema maya di cui qui si è parlato nel § 3.2 (ma si può anche obiettare che, dopo tutto, *un punto* è ormai un segno convenzionale per lo zero e dunque il sistema *gobar* utilizza una sorta di zero non *a fianco* delle cifre significative ma *al di sopra*, come esemplificato nella didascalia della figura 10 [cfr. del resto la discussione della questione in Cajori 1928, pp. 53-54]). Non deve comunque stupire che in Gerberto e nei suoi immediati continuatori lo zero *non* compaia: esso «comincia a svolgere il suo ruolo fondamentale solo

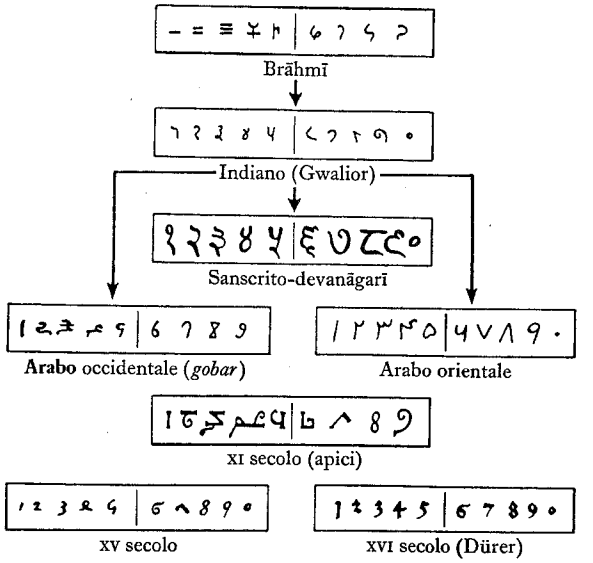


Figura 10.

La genealogia delle nostre cifre «indo-arabiche» [cfr. Menninger 1957, trad. ingl. p. 418; Boyer 1968, trad. it. p. 277]. La «migrazione verso occidente» è così immediatamente visualizzata: dalle lettere brāhmī per le prime nove cifre (da cui si ipotizza siano derivati i segni indiani) si ha la notazione indiana cui va aggiunto il simbolo zero. Il lettore potrà inoltre agevolmente confrontare le due forme «arabo-orientale» e «arabo-occidentale». Nel sistema *gobar* manca un esplicito simbolo di zero, ma, come si è detto a p. 1331, nei manoscritti viene adottata la convenzione per cui dei punti posti sopra le cifre indicano gli «ordini»: un punto le decine, due punti le centinaia, ecc. (è dunque un espediente per molti versi analogo a quello maya esemplificato nella figura 5): così 4̈ 5̈ 6 è il nostro 456, mentre 4̈ 5̈ è il nostro 450, e 4̈ 6 il nostro 406, ecc. Sotto le due versioni arabe è riportato il discusso sistema degli apici. Infine le due ultime scritture dànno due versioni delle nostre cifre decimali notevolmente successive alla «rivoluzione culturale» promossa fin dal secolo XIII dagli «algoristi». Occorre dire che questi riuscirono a imporsi sugli «abacisti» in modo definitivo solo nel secolo XVI.

con dei calcoli scritti; poiché Gerberto e i suoi discepoli non avevano conoscenza di tali calcoli, non erano in grado di afferrare l'essenza dei "nuovi" sistemi di numerazione. Si limitarono ad adottare i simboli, la cui origine misteriosa e il cui significato erano offuscati dai loro oscuri nomi [cfr. la didascalia alla figura 9], alcuni d'origine araba... Ci s'imbatte qui in un punto assai istruttivo della storia culturale dei numeri. Il sistema perfezionato e maturo per scrivere i numeri che gli Arabi ormai possedevano e che doveva in futuro rivelarsi cosí essenziale per l'Occidente, venne adottato già nel primo medioevo, *ma in modo cieco*... La nuova acquisizione rimase morta, perché il suo spirito non venne compreso» [Menninger 1957, trad. ingl. p. 325]. È sempre con gli occhiali di una tradizione che si leggono e si *intro*ducono (o *tra*ducono) acquisizioni di altre tradizioni, come piú volte si è detto nelle pagine di questa stessa *Enciclopedia* (cfr. in particolare gli articoli «Matematiche», «Paradigma» e «Scienza»). Forzando un po' le cose, si potrebbe dire che i Latini discepoli di Gerberto, se anche si fossero imbattuti in uno zero, non lo avrebbero riconosciuto come tale, ovvero, semplicemente non avrebbero saputo cosa farsene.

4. *Il «molto» e il «niente».*

Complessivamente, «la situazione, per quanto riguarda l'introduzione delle cifre numeriche in Europa, è altrettanto confusa quanto quella che circonda l'invenzione di tale sistema forse mezzo millennio prima. Inoltre, non è chiaro che vi sia stato uso continuo delle nuove cifre in Europa nei due secoli successivi a Gerberto; infatti è soltanto nel XIII secolo che il sistema indo-arabico venne definitivamente introdotto in Europa, e ciò per opera non di un solo uomo, ma di parecchi» [Boyer 1968, trad. it. p. 292]. Le modalità di questa diffusione, in un contesto profondamente diverso da quello dei tempi di Gerberto, sono state analizzate in opere ormai classiche [come per esempio Hill 1915; Smith e Karpinski 1911; per un quadro della diffusione del sistema indiano, non solo, tramite gli Arabi, in Occidente, ma «mondiale», si veda l'esauriente Ifrah 1981, pp. 487-518]. Qui basterà ricordare che mentre il sistema indo-arabico veniva spiegato ai lettori latini da un Adelardo di Bath, pressappoco negli stessi anni ʾAbrāhām ibn ʿEzrā, vissuto tra il 1092 e il 1167, introduce un analogo schema di numerazione: le prime nove cifre alfabetiche ebraiche indicano i numeri da 1 a 9, mentre un circoletto denota lo zero. Allo stesso modo nella cultura matematica bizantina un segno speciale per lo zero si aggiunge alle prime nove cifre alfabetiche greche.

Lo zero ha quindi raggiunto piena cittadinanza? Alessandro De Villa Dei, che insegna a Parigi verso il 1240, cosí inizia il suo *Carmen de Algorismo*: «Hinc incipit algorismus. | Haec algorismus ars praesens dicitur in qua | talibus indorum fruimur bis quinque figuris | 0 9 8 7 6 5 4 3 2 1» [citato in Menninger 1957, trad. ingl. pp. 412, 415]. L'ordine rovesciato delle dieci cifre, comune anche a altre delle prime presentazioni latine, è tipica traccia dell'archetipo arabo.

Ma i dubbi e le perplessità circa lo zero traspaiono dalla stessa varietà dei vocaboli coniati (cfr. del resto quanto osservato a proposito della nomenclatura indiana a p. 1326). È molto istruttivo, per esempio, scorrere il capitolo che Smith e Karpinski gli dedicano: «Il nome di questo importantissimo simbolo richiede un po' di attenzione, – scrivono i due autori, rivolti particolarmente a lettori di lingua inglese, – per il fatto stesso che anche ai nostri giorni resta una certa indecisione. Ne parliamo infatti come *zero*, *naught* o anche *cipher*; il centralino telefonico lo chiama spesso *O*, mentre la persona illetterata o semplicemente trascurata lo chiama *aught*» [1911, p. 56].

Si può quindi immaginare la Babele del passato. Tanto per fare un esempio, uno dei pionieri di quello che verrà considerato il punto di vista degli «algoristi» (cioè degli esperti del calcolo scritto in contrapposizione agli esperti dell'arte dell'abaco o «abacisti»: due punti di vista contrapposti – il lettore li trova esposti rispettivamente negli articoli «Abaco» e «Calcolo» della presente *Enciclopedia* – tra cui non è mancata però anche una certa commistione), l'astronomo e matematico inglese del XIII secolo John Holywood (Giovanni di Sacrobosco) scrive nel suo *Algorithmus*: «Sciendum quod iuxta 9 limites 9 inveniuntur figurae significative 9 digitos representantes qui tales sunt 0 9 8 7 6 5 4 3 2 1 decima dicitur vel circulus vel cifra vel figura nihil quoniam nihil significat, ipsa tamen locum ten/n/ens (?) dat aliis significare, nam sine cifra vel cifris purus non potest scribis articulus» [citato e discusso in Menninger 1957, trad. ingl. pp. 402-3].

L'archetipo è, ovviamente, il sanscrito *śūnya*. Esso viene reso in arabo *as-ṣifr* o *ṣifr*, da cui il latino *cifra* (cfr. fig. 11). Si legge nel *Carmen* di Alessandro De Villa Dei: «Cifra nil significat, dat significare sequenti» [citato *ibid.*, p. 423]. Massimo Planude (1330), che scrive sotto influenza sia greca sia araba, lo rende con τζίφρα (e non è il solo [cfr. le osservazioni di Smith e Karpinski 1911, p. 57, nota 4]). Alla medesima parola *as-ṣifr* si riconducono in

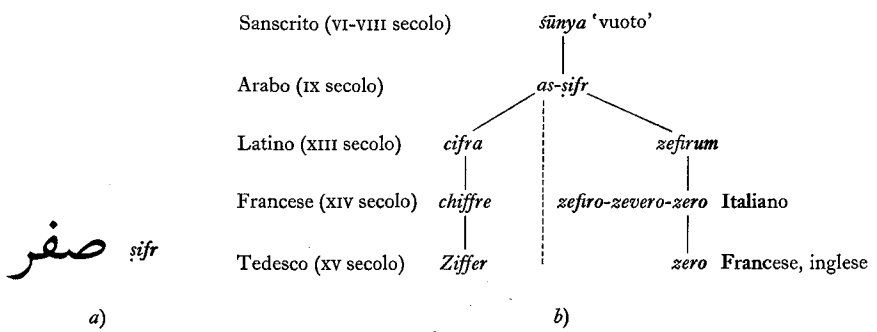


Figura 11.

a) Il termine arabo per zero [cfr. Ifrah 1981, p. 509]. *b*) Uno schema (non completo) per la genealogia dei termini piú in uso per denotare lo zero, in particolare del termine 'zero' stesso [Menninger 1957, trad. ingl. p. 401].

modo naturale l'inglese *cipher* e il francese *chiffre*; ma in italiano *cifra* non denota specificamente lo zero, e una situazione analoga si produce in altre lingue. Non mancano dunque usi ambigui: ancora Johann Huswirt, nel suo *Enchiridion Algorismi* (Köln 1501) usa *cifra* sia come zero sia come semplice numero che dà per zero i quattro appellativi del Sacrobosco: *theca*, *circulus*, *cifra* e *figura nihili* [cfr. *ibid.*, p. 58].

E si potrebbe ancora continuare. Ma basterà qui ricordare che è Leonardo Pisano, nel *Liber abaci* (1202), che conia il termine *zephirum*; in un trattato di aritmetica scritto in italiano da Jacopo fiorentino, circa un secolo dopo (1307), compare la forma *zeuero*: «Et doveto sapere chel zeuero per se solo non significa nulla ma è potentia di fare significare... Et decina o centinaia o migliaia non si puote scrivere senza questo segno o» [citato e discusso in Smith e Karpinski 1911, p. 58, nota 1]. Due paiono essere stati gli schemi di derivazione per la parola 'zero': 1) *zefiro*, *zeviro*, *zeiro*, *zero*; e 2) *zefiro*, *zefro*, *zevro*, *zero* [Jordan 1905]. La prima opera a stampa in cui compare la forma finale *zero* è l'aritmetica di Calandri del 1491: «Sono dieci le figure con le quali ciascun numero si può significare: delle quali n'è una che si chiama zero; et per se sola nulla significa» [citato e discusso in Smith e Karpinski 1911, p. 59]. Ma zero già si trovava nei manoscritti della metà del XIV secolo [*ibid.*]; si diffonderà comunque anche fuori d'Italia, per esempio in Francia e in Inghilterra (cfr. ancora la figura 10).

Elemento unificante delle citazioni qui riportate è ancora quella natura paradossale dello zero cui si è accennato a pp. 1320-21: zero – *nulla figura* o *nulla* come è spesso chiamato – di per sé nulla significa (dunque: significa *nulla*, dunque *qualcosa* obietterebbe un Fredegiso che fosse al corrente dell'«arte» insegnata dal «philosopho Algo»), ma scritto opportunamente dopo una cifra significativa ne aumenta il valore. Fino a che punto è dunque una cifra come tutte le altre? Se non si vuole ammettere che sia un segno (un segno per il nulla), è una semplice mancanza. Dunque non è una cifra. «Come l'asino vorrebbe essere un leone e la scimmia una regina, cosí lo zero si dà arie e pretende di essere una cifra», si trova scritto ancora sul finire del Quattrocento [citato in Menninger 1957, trad. ingl. pp. 422-23]; e nel 1514 il matematico tedesco Köbel parla di nove *bedeutlichen Figuren* 'cifre denotanti' contrapposte al solo *Zeiffer* 'zero': «Ringlein *O*, die Ziffer genannt, die nichts bedeut» [citato e discusso *ibid.*, pp. 402-3]. Nel *King Lear* [I, IV] la natura imbarazzante e paradossale dello zero spicca nelle parole del Matto a Lear: «Now thou art an o without a figure: I am better than thou art now; I am a fool, thou art nothing» («Adesso sei uno zero a sinistra. Ora io sono piú di te; io sono un matto e tu un niente»). Zero *o* pazzia, dunque? E perché non zero *e* pazzia? Come si legge, a proposito del matto dei tarocchi: «Noi, questo Atout, lo chiamiamo ZERO, ancorché venga situato, nel Gioco, dopo il XXI, considerando che non conta quando è solo, e non ha che il valore che conferisce alle altre Carte, esattamente come il nostro zero: come a dimostrare che nulla è in grado di esistere senza la Follia» [Court de Gébelin 1773-82, trad. it. p. 24].

5. *La «setta dei neminiani». Il contesto dell'algebra e dell'analisi.*

A proposito della «tentazione» di trattare termini come 'zero', 'nulla', ecc. come se denotassero «enti fuori dall'ordinario dotati di una sorta di misteriosa esistenza», Max Black trova un curioso precedente «nella setta detta dei *Neminiani*» fiorita sul finire del XIII secolo, cosiddetta da coloro che «adoravano *Nemo* (cioè nessuno), la persona cui supponevano si riferisse quel termine nei testi biblici e classici» [1977, p. 771] e insinua che non pochi filosofi, per esempio «esistenzialisti come Martin Heidegger», nel trattare *la questione metafisica del nulla* si ritrovano, per cosí dire, a ripercorrerne le orme. Non si vuole, in questa sede, discutere quest'ultima tesi; ci si limiterà invece ad osservare che proprio quella profonda rivoluzione intellettuale con cui si è imposto in Occidente il punto di vista degli «algoristi» (cioè una notazione posizionale provvista di o come strumento di calcolo *scritto*) in un intreccio molto forte di vita civile e pratica matematica (cfr. quanto osservato *passim* nel citato articolo «Calcolo») ha posto le premesse della considerazione dello zero come un ente matematico, anche se non della sua... adorazione.

Black caratterizza il simbolo o come qualcosa che «non sta per qualche entità peculiare o misteriosa, anche se vi sono modi ben specifici di usarlo»: dopo tutto si è trattato di «uno strumento ausiliare, impiegato per una semplice assenza, [che] via via ha preso l'apparenza di un simulacro di sostanza, che sembra stare per un vero numero» [*ibid.*, p. 770]. A secoli di distanza da chi beffeggiava zero paragonandolo, come si è visto, all'asino che vuol essere leone o alla scimmia che vuol essere regina la storia dello zero sarebbe dunque, ancora, la *storia di una sorta di usurpazione...*

Nulla da obiettare. Purché si tenga conto che non poche altre estensioni del concetto di numero sono allo stesso titolo «usurpazioni», «sfide al senso comune», «atti violenti», ecc.: il «calcolo dei profitti e delle perdite», ad esempio, motivava l'introduzione dei numeri «con segno» (o «numeri relativi») ma per lungo tempo i numeri negativi restano semplici segni dell'impossibilità di calcolare (in termini di naturali) differenze tipo $1-2$, $3-5$, ecc. e vennero abitualmente chiamati *numeri ficti*; già con i grandi algebristi del Cinquecento era emersa l'utilità dei numeri complessi nel maneggiare equazioni algebriche a coefficienti reali, ma per molto tempo ancora la «radice di meno uno» non doveva essere altro che una *nota inexplicabilis*, semplice *pro memoria* del fatto che un'apparentemente semplice equazione come $x^2+1=0$ non ammette «in realtà» soluzione; gli stessi irrazionali se non venivano respinti «fuori dai numeri», come volevano i piú radicali tra i «rigoristi» della matematica greca, dovevano venir giustificati sulla base di intuitive considerazioni «di continuità» prima di trovare una spiegazione soddisfacente gli standard di rigore...

Eppure questo «sviluppo illogico di una materia logica» (per usare una felice espressione di Kline [1980, p. 100]), si è rivelato, come è noto, proficuo almeno sotto tre aspetti: l'approfondimento della problematica concernente la successione dei naturali, la pratica del calcolo, la modellizzazione matematica

dei processi reali (questi tre aspetti sono trattati negli articoli «Numero», «Modello» e «Calcolo» in questa stessa *Enciclopedia*). Sotto tutti e tre questi punti di vista l'introduzione dello zero ha rappresentato un'importante innovazione. Già della pratica del calcolo si è detto ampiamente nei paragrafi precedenti: alcuni aspetti calcolistici, legati al dominio dell'algebra e dell'analisi, verranno però ripresi in questo paragrafo. Nel § 6 si affronterà invece la questione dello zero dal punto di vista dell'assiomatica dei numeri naturali e della stessa teoria degli insiemi (e ricompariranno in questa occasione le ombre dei Neminiani e il realismo logico-linguistico di Fredegiso); nel § 7 il riferimento allo zero (o meglio alla «classe vuota») permetterà un'esplicazione dei cosiddetti «zeri puri di esistenza».

5.1. Gruppi e anelli.

Si assumerà nel seguito che il lettore sia familiare con l'usuale ricostruzione degli interi relativi **Z** e delle frazioni **Q** a partire dai naturali **N** (zero incluso), nonché con le teorie dei reali **R** e dei complessi **C** che dopo la «rigorizzazione» ottocentesca sono entrate a far parte delle basi dell'edificio delle matematiche. (Tali argomenti sono del resto ampiamente svolti in altri articoli della presente *Enciclopedia*, in particolare «Calcolo» e «Insieme»). Per economia di pensiero e comodità di linguaggio nelle pagine immediatamente successive ci si muoverà entro la cornice «strutturale» (delineata nell'articolo «Strutture matematiche» della presente *Enciclopedia*) come quella che assai adeguatamente oggi si presta alla presentazione delle proprietà algebriche che qui interessano.

Nell'abaco, zero è semplicemente un posto vuoto (come del resto era una scatola vuota nella realizzazione concreta data nel § 1; cfr. fig. 12); nell'aritmetica di **Z** (come già si è detto a proposito dei matematici indiani) può venir preso da solo: esso è un elemento di **Z** come gli altri, se pur dotato di notevoli proprietà.

Si consideri ora la semplice operazione di addizione in **Z**: la somma di due interi relativi è ancora un intero relativo, valgono le proprietà associativa e

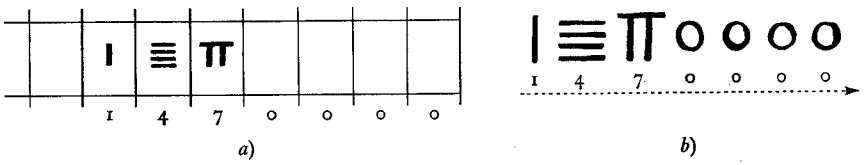


Figura 12.

Evoluzione della notazione cinese. In una prima fase il sistema cinese (a base dieci, almeno dalla nostra era cristiana in poi) ignora però lo zero: i simboli sono posti entro caselle, in certi casi lasciate «vuote», a somiglianza di come si opera con l'abaco (*a*). Con l'influenza indiana si passa però a una notazione posizionale provvista di zero (*b*) [Ifrah 1981, pp. 487 e 488; per la diffusione dello zero nell'Estremo Oriente cfr. *ibid.*, pp. 487-89].

commutativa, inoltre se si somma un qualsiasi intero con zero dà ancora quell'intero e per ogni intero è possibile definire «l'inverso» (quello che abitualmente si chiama «l'opposto») che sommato con quell'intero dà zero. In particolare zero è l'opposto di se stesso. Si è cosí descritta una realizzazione «concreta» di una fondamentale struttura «astratta»: quella di gruppo (commutativo). Ora in qualsiasi gruppo (commutativo) zero funziona da «elemento neutro» rispetto alla «legge di composizione considerata». L'unicità dello zero in **Z** si ritrova in ogni gruppo, sotto un profilo del tutto generale. Si supponga infatti che in un gruppo (commutativo) 0 e 0^* siano due elementi neutri: dunque, per ogni elemento a del gruppo valgono le equazioni seguenti (dove la legge di composizione, seguendo la cosiddetta notazione additiva, è ancora indicata da $+$): $a+0=a$ e $a+0^*=a$. In particolare sarà $0^*+0=0^*$ e $0+0^*=0$ onde per la commutatività $0^*=0$ (è possibile, peraltro, dimostrare l'unicità dell'elemento neutro anche per gruppi *non* commutativi).

È bene ribadire che dimostrazioni come quelle testé riportate valgono per un'infinità di realizzazioni della struttura astratta di gruppo (in cui anche certe strutture «degeneri» non sono del tutto prive d'interesse; cfr. la scherzosa esemplificazione della figura 13). Ma si sposti ora l'attenzione su una struttura piú ricca di quella di gruppo, cioè quella di anello e si pensi ancora a **Z**, ma questa volta con le due leggi di composizione rappresentate dall'usuale addizione e moltiplicazione. In linea generale l'elemento neutro del gruppo additivo di un anello viene ancora chiamato zero e per ogni elemento a dell'anello si ha $a+0=a$ e $a\cdot 0=a$. Queste non sono altro che le generalizzazioni delle due leggi (3) e (1) di p. 1328. Ma entro il contesto della trattazione assiomatica delle strutture, le due proprietà hanno un peso diverso. La prima non è altro che la definizione dello zero come elemento neutro dell'addizione; la seconda viene invece ricavata dalla proprietà distributiva. Infatti, da $0+0=0$ si ha:

$$a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$$

Ora, $a\cdot 0$ risolve l'equazione $a\cdot 0+x=a\cdot 0$; ma anche 0 risolve tale equazione e, poiché in un gruppo (ogni anello è un gruppo commutativo rispetto alla sola «addizione») equazioni siffatte possiedono una sola soluzione, segue $a\cdot 0=0$.

5.2. I corpi e la divisione per zero.

In un anello equazioni del tipo $0\cdot x=b$ con $b\neq 0$ sono dunque insolubili: questo aspetto assume piena rilevanza quando si fissa assiomaticamente la possibilità della divisione e ci si restringe a quei particolari anelli che costituiscono i cosiddetti corpi o campi. L'importanza di queste ultime strutture (si pensi ai numeri razionali **Q**, ai numeri reali **R** e ai numeri complessi **C** con leggi di composizione rappresentate dalle usuali addizione e moltiplicazione) difficilmente potrebbe essere sottovalutata nelle matematiche. È proprio in questo contesto che si ritrova sotto un profilo generale la questione della divisione per zero.

Figura 13.

La «neotomatica» del gufo della strip di *Pogo Possum* (Walt Kelly, 1965 [«Linus», I (1965), 3, pp. 57 e 58]). Tra le leggi della «neotomatica» compaiono tra l'altro le relazioni $0 \times 0 = 0$ e $0 + 0 = 0$, che rappresentano un gruppo «degenere» di un solo elemento (cioè l'elemento neutro) in notazione moltiplicativa, rispettivamente additiva.

Pare che Aristotele facesse notare che non si può dividere un numero come quattro per il «nulla» [cfr. Boyer 1943]; niente da obiettare, finché il «nulla» non è un numero. Ma ora che zero è un numero come tutti gli altri?

Ci si collochi al livello di generalità costituito dalla teoria dei corpi (commutativi). Come immediatamente si evince dagli assiomi elencati nell'articolo «Calcolo», qui piú volte citato (II, p. 393), gli elementi *diversi dallo zero* formano un gruppo (commutativo) rispetto all'operazione di moltiplicazione: in particolare il sesto degli assiomi ivi elencati sancisce l'esistenza di un «inverso» moltiplicativo (il cosiddetto «reciproco») solo per elementi diversi dallo zero: poiché la divisione è definita ricorrendo al reciproco del divisore, sembra che non ci siano strade per la divisione per zero. Che dire allora di «leggi» come la (2) di p. 1328? Perché di essa non viene fornita una generalizzazione come si è fatto per la (3) e per la (1)? La ragione può essere trovata nel modo seguente: si supponga, per esempio, $1/0 = 1$; si è ancora disposti a moltiplicare entrambi i membri di questa uguaglianza per uno stesso elemento, per esempio in particolare zero, e concludere $1 = 0 \cdot 1 = 0$, quando sappiamo $1 \neq 0$? «Che anche in matematica ogni cosa non è proprio la migliore in questo mondo che pure è il migliore dei mondi possibili, lo ricorda proprio la *vexata quaestio* della definizione della divisione» [Suppes 1957, p. 163].

Scartata la soluzione proposta fin dai tempi di Mahāvīra, si aprono altre possibilità. Senza ricostruirne l'origine e la storia, ma con l'occhio rivolto piuttosto ai problemi matematici, logici e linguistici sottostanti, si distingueranno [cfr. *ibid.*, pp. 163-69] cinque differenti approcci alla divisione per zero: tutti e cinque cattureranno, come si avrà modo di constatare, *alcuni* aspetti rilevanti della pratica matematica e corrisponderanno a differenti «metafisiche del calcolo».

1) *Tagliare il nodo gordiano*: ovvero espressioni come $1/0 = 1/0$ non hanno significato. È forse la soluzione piú drastica, quella apparentemente piú semplice, quella che pare implicitamente suggerita da non pochi manuali quando si esplicita il «divieto» della divisione per zero. Eppure cosí facendo si insinua una nuova difficoltà, poiché non pare agevole (o addirittura possibile) decidere sempre circa la «significanza» delle espressioni. In **R** si consideri ad esempio [cfr. *ibid.*, p. 166] per ogni naturale n diverso da zero l'espressione

$$\frac{1}{n^*} = \frac{1}{n^*} \tag{5}$$

ove n^* è definito come segue: $n^* = 1$ se n è dispari o se n è pari e somma di due numeri primi; $n^* = 0$ se n è pari e non è somma di due primi. Poiché l'esistenza di numeri pari che non sono somma di due primi è un problema di teoria dei numeri ancora aperto (congettura di Goldbach), rimane aperta, alla luce di quanto sopra, la significanza (non la falsità o la verità!) di un'espressione come la (5).

2) *Definizione «condizionale» della divisione*: ci si limita a **R**. $x/0$ è un numero reale, ma la divisione viene definita ricorrendo a una «definizione condizionale»: se $y \neq 0$ allora $x/y = z$ se e solo se $x = y \cdot z$. Cosí facendo per ogni

x, $x/0$ è un numero reale, ma non si è in grado di indicare *quale* elemento sia. Conseguentemente non si possono decidere asserti tipo

$$(6) \qquad \frac{1}{0} = \frac{2}{0}$$

ecc.

3) *Definizione indipendente dagli assiomi*: sempre in **R**, per eliminare quest'ultimo inconveniente, si può definire $x/0 = 0$ per ogni x. La definizione della divisione suona allora:

$$\frac{x}{y} = z \leftrightarrow (y \neq 0 \rightarrow x = y \cdot z) \,\&\, (y = 0 \rightarrow z = 0)$$

La divisione è estesa a ogni numero reale nullo o non nullo. Per molti versi pare dunque un approccio piú soddisfacente, in quanto la definizione della divisione è «indipendente dagli assiomi» cioè «non richiede alcun teorema che la giustifichi» [Suppes 1957, p. 164].

È la via che, sul piano generale, può venir seguita in qualsiasi corpo: ogni elemento del corpo x ammette ora inverso moltiplicativo che viene definito come quell'y per cui $x \times y = 1$ per $x \neq 0$ e come 0 per $x = 0$. Ne consegue che per decidere la verità o la falsità di espressioni tipo $x \times x^{-1} = 1$ ove x^{-1} abbrevia il reciproco di x per *qualsiasi* x del corpo occorrerà considerare una ulteriore condizione (se x sia o no diverso da zero). Complicazioni del genere sono spia di un fatto abbastanza profondo dal punto di vista algebrico: al contrario di gruppi e anelli, i corpi non sono «algebre» nel senso ristretto del termine, cioè, detto piú precisamente, non possono venir completamente descritti servendosi solo di equazioni (la classe dei corpi, per utilizzare la terminologia di Tarski, non è una «classe definibile con equazioni» o, come altri dice, «una varietà» [cfr. per esempio Cohn 1965, trad. it. in particolare pp. 72-73, 186 sgg. e ancora pp. 214 sgg.]).

4) *I corpi come strutture relazionali*: appare allora abbastanza naturale, anche se poco confacente alla pratica abituale, sostituire ai simboli per operazioni simboli per relazioni. Il simbolo 0 viene allora sostituito dal predicato a un posto Z (ovvero $Z(x)$ vuol dire che x è l'elemento neutro per l'addizione, cioè zero), un predicato a tre posti S sostituisce il simbolo $+$, un predicato a tre posti M sostituisce il simbolo $\times$, ecc. negli usuali assiomi dei corpi. L'operazione di divisione si può allora definire, eliminando gl'inconvenienti di 1), 2) e 3) per esempio cosí:

$$D(x, y, z) \leftrightarrow \neg Z(y) \,\&\, M(y, z, x).$$

5) *Ampliare il dominio*: data l'importanza che ha avuto nello sviluppo di non poche idee matematiche, vale però la pena di accennare a un quinto approccio, limitandosi di nuovo al caso dei numeri reali. Mantenendo l'usuale notazione per le operazioni fondamentali, si può introdurre un simbolo R come un predicato a un posto che significa appunto «essere un numero reale» e riformulare i tradizionali assiomi in modo che si possa esprimere che la somma e

il prodotto di due numeri reali sono ancora numeri reali. In questo modo l'introduzione del predicato R amplia il dominio: ora, infatti, non è detto che *tutte* le entità del dominio in cui s'interpretano le espressioni del linguaggio siano numeri reali; in particolare non è detto che $1/0$ sia un numero reale!

Si potrà definire la divisione nel modo seguente:

$$[R(x) \,\&\, R(y) \,\&\, R(z) \,\&\, y \neq 0] \rightarrow [x/y = z \leftrightarrow z = y \cdot z]$$

Per questa via non si dimostra né che $x/0$ è un numero reale né che $x/0$ non è un numero reale, «ma non si è nemmeno costretti alla situazione contro intuitiva di chiamare numero reale $x/0$» [Suppes 1957, p. 168].

5.3. Dallo zero all'infinito.

Si consideri ancora per qualche istante il quinto approccio alla divisione per zero trattato nel § 5.2. Si introduca nel sistema cosí delineato un oggetto che *non* è un numero reale, poniamo ν, formulando l'assioma $\neg R(\nu)$.

Si modifichi quindi la definizione della divisione data piú sopra cosí:

$$[R(x) \,\&\, R(y)] \rightarrow [x/y = z \leftrightarrow [(y \neq 0 \rightarrow R(z) \,\&\, \\ \&\, (x = y \cdot z)) \,\&\, (y = 0 \rightarrow z = \nu)]].$$

In questo modo non solo $x/0$ è escluso dal dominio dei reali, ma, se x e y sono reali e pure è $x \neq y$, si ha $x/0 = y/0$, con il che si vieta la proliferazione di «strani» enti matematici.

Nel reale sviluppo storico delle matematiche mosse analoghe sono state di fatto e piú volte compiute. Per esempio il passaggio all'infinito *via* la divisione di un usuale numero finito per zero è un archetipo che si è già visto operante in Bhāskara. Lo si ritrova apertamente teorizzato – con pochi scrupoli verso il rigore matematico – nell'*Algebra* [1770] di Eulero: qui egli pone $\infty = 1/0$; ma non compie affatto l'ultimo passo implicito nella ridefinizione della divisione data poche righe piú sopra; anzi gli pare naturale che $2/0$ sia 2∞, cioè il doppio di $1/0$. Inoltre nelle considerazioni fin qui fatte su ν non si è ancora alluso al fatto che **R** è un corpo ordinato (cfr. ancora il citato articolo «Calcolo» alla p. 396) e si è tacitamente assunto che l'usuale ordinamento continui a valere relativizzato a R [cfr. Suppes 1957, p. 167]. Nulla si dice a proposito del posto di ν rispetto alla usuale relazione d'ordine. Ma se s'identifica ν con l'infinito? Se per ν, ovvero per ∞, si istituisce un calcolo o se si considera, poniamo, $+\infty$ come maggiore di ogni numero (finito) positivo e $-\infty$ minore di ogni numero (finito) negativo?

Qui si è al centro della «palude dell'analisi» (per usare la pittoresca espressione di Kline [1980]). Detto in modo molto schematico: *a*) la divisione per zero di un qualsiasi numero usuale (cioè «finito») giustifica l'introduzione dell'infinito [cfr. a questo proposito la discussione in Couturat 1896, pp. 277-91]; *b*) la divisione per l'infinito di un qualsiasi numero finito è anch'essa lecita; *c*) curiosamente, non si riottiene da quest'ultima operazione zero, ma una nuova entità, una quantità «minore di ogni quantità finita assegnabile» ma «di-

versa da zero», cioè un infinitesimo. Ora, in altri articoli della presente *Enciclopedia* (in particolare «Calcolo», «Differenziale», «Infinitesimale» e «Infinito» e, per aspetti piú generali, «Matematiche») la questione dell'infinito e dell'infinitesimo nelle matematiche è stata ampiamente trattata: qui ci si limiterà ad osservare che la strategia piú sopra sommariamente schematizzata può venir vista sia come un volgare «trucco», come avrebbe detto qualsiasi rigorista, o come un «enigma», come avrebbe riconosciuto uno di quegli analisti incoraggiati dai successi ma sconcertati dall'oscurità dei fondamenti; comunque essa rappresenta una problematica tipicamente «mal strutturata» che però si rivela, sul lungo periodo, una «matrice» di *buoni* problemi [per gli aspetti generali di questa tematica, cfr. quanto osservato nell'articolo «Ricerca» in questa stessa *Enciclopedia*; sulla questione cfr. ancora Morini 1980, pp. 191-93].

Ovviamente lo schema *a*), *b*), *c*) è solo un abbozzo di come gli infinitesimi possono venir introdotti nel calcolo. Ben piú sofisticate metafisiche (cioè «metafisiche applicate» come specificato nel § 3 dell'articolo «Metafisica» in questa stessa *Enciclopedia*) furono di fatto messe all'opera: dalla concezione newtoniana delle «flussioni» e delle «fluenti» alla teoria leibniziana dei «differenziali» giustificati ricorrendo alla legge della continuità, alla «teoria degli zeri» di Eulero (polemicamente rivolta contro «i sofismi dei monadisti»).

In questa sede si vuole ancora insistere solo su un aspetto che di nuovo allo zero rimanda. Per fare un esempio classico, si supponga di calcolare – *via* infinitesimi, giustificati in nome di Newton o di Leibniz qui non importa – la derivata della funzione $y=x^2$. Sulla curva corrispondente nel piano cartesiano si considera allora il punto di coordinate (x, x^2). Se x varia per un incremento *infinitesimo* dx, allora

$$dy=(x+dx)^2-x^2=2x\,dx+(dx)^2.$$

Dividendo per dx si ottiene

$$\frac{dy}{dx}=2x+dx$$

e poiché dx è infinitesimo si ha pure

$$\frac{dy}{dx}=2x.$$

Ed è un altro modo di «truccare le carte»: dx è assunto diverso da zero nel primo passo (divisione per dx di entrambi i membri di un'equazione) e uguale a zero nel secondo (posizione di $2x+dx$ come uguale a $2x$). Proprio espedienti del genere censurava implacabilmente il vescovo Berkeley, polemizzando sia con Newton sia con Leibniz, là dove riteneva inammissibile dare al medesimo simbolo (il dx di cui sopra) un «doppio significato», compiendo in questo modo «un sofisma manifesto» [1734, in particolare § 15, e anche §§ 25, 26 e 27]. Ma se Berkeley riteneva che il calcolo deviasse dal retto cammino della «dimostrazione scientifica» per diventare *a knack*, *an art*, *an artifice*, due anni dopo il reverendo Bayes gli ribatteva che «in quel modo di ragionare» non c'era in

realtà alcuna fallacia: in un calcolo come quello appena esposto, dx e quindi $2x+dx$ sono considerati «a tempi diversi»: non c'è dunque nessuna incoerenza nel supporre «in tempi diversi» $2x$ e $2x+dx$ prima disuguali e poi uguali: «E c'è da meravigliarsi che un fine ragionatore come il nostro Autore [Berkeley] non sia in grado di distinguere fra tempi diversi» [1736, p. 39]. E conclude: «Se supponiamo [due quantità] prima disuguali e poi divenire uguali, non c'è piú ombra di difficoltà in ciò. E non c'è nulla di strano nel fatto che dalla supposizione di queste due cose che accadono l'una dopo l'altra, posso dedurre una conclusione che non seguirebbe dall'una o dall'altra supposizione presa per sé» [*ibid.*, p. 40].

Nella concezione «dinamica» di Bayes, dunque, «quantità» diverse da zero possono *diventare* zero. Ma si confronti questa posizione con le mosse di coloro che sul Continente reagiscono alle critiche. Per esempio, Eulero, in particolare nelle sue *Institutiones calculi differentialis* [1755], opera un notevole slittamento da (e contro) Leibniz. Quel dx che Leibniz considerava un infinitesimo per Eulero è semplicemente zero: non c'è, dunque, «trucco». Conseguentemente dy/dx che per Leibniz era il rapporto di due infinitesimi, è per Eulero in realtà $0/0$. Solo che per Eulero questo simbolo scritto come *rapporto di due nulla* può assumere vari valori!

Si veda il ragionamento di Eulero piú in dettaglio: come già si è piú volte ripetuto, per ogni numero n è $n\cdot 0=0$: *se si divide per zero* si ottiene allora $n=0/0$. In questo modo viene «giustificato» l'abituale procedimento di calcolo della derivata di una funzione, per esempio quello che da $y=x^2$ ha ricavato $dy/dx=2x$. Quel che per Leibniz restava sempre un infinitesimo diverso da zero (e Leibniz doveva poi giustificare perché si potesse mai passare da $2x+dx$ a $2x$) *diventava* zero per Eulero e, diventando zero anche dy, risultava uguale a $2x$ il rapporto $0/0$.

Cosí nella «teoria degli zeri» di Eulero trovava un importante ruolo euristico la forma simbolica $0/0$, impiegata anche da altri matematici come d'Alembert, ma già rifiutata da Lagrange e da Carnot; proprio tale forma verrà a costituire «il piú temibile di tutti i simboli o enigmi del calcolo differenziale» [Bledsoe 1867, p. 215], a rappresentare quindi «il campo di battaglia delle scuole di pensiero rivali a proposito del calcolo» [Cajori 1929, p. 261], per finire infine come una semplice e relativamente innocua abbreviazione in qualche testo di analisi *dopo* la rivoluzione del rigore promossa da Weierstrass.

È facile del resto, col senno di poi, relegare nel cimitero delle concezioni prescientifiche (se non antiscientifiche) le intuizioni di Newton e dei suoi difensori, o di Leibniz e dello stesso Eulero. La concezione che si è imposta con Weierstrass ha ritrovato per altra via i grandi risultati ottenuti *via* infinitesimi e ha fatto sí che anche in analisi l'infinito (e l'infinitesimo) si riducesse a *façon de parler*. Tuttavia, come è ampiamente mostrato nell'articolo «Infinitesimale», questo drastico giudizio va non poco ridimensionato. Infine, in un adeguato contesto come quello fornito dall'analisi «non standard» di Robinson e Luxemburg (cfr. il citato articolo «Infinitesimale», § 3), gli infinitesimi vengono ritrovati come elementi della «monade» dello 0 reale: essi quindi *non* sono zero

(e la divisione per zero è, ovviamente, anche qui interdetta) ma la loro «vicinanza» con lo zero è soddisfacentemente chiarita dallo studio delle proprietà dell'«allargamento» non standard **R*** di **R**.

6. *Lo zero di Peano, l'insieme vuoto e la classe nulla.*

6.1. Gli assiomi di Peano per i numeri naturali.

Una volta messe in luce le proprietà algebriche dello zero e, al contempo, tenendo conto delle estensioni del concetto di numero a partire dai naturali, le pagine che seguono s'incentreranno sulla definizione dello zero dei naturali, e anzitutto sulla formulazione assiomatico-formale fornita da Peano nelle varie edizioni del suo *Formulaire*. Gli assiomi peaniani sono stati piú volte trattati nella presente *Enciclopedia* (cfr. per esempio l'articolo «Calcolo», ove compaiono con la sigla P.1-P.5 alla p. 408): essi, come è noto, utilizzano tre idee *non definite* che sono appunto *numero* (come abbreviazione di numero naturale), *zero* e *successore*. In tale sistema zero è dunque qualcosa, il primo dei numeri, ma determinare *che cosa* è un altro problema!

È lo stesso Peano che nel *Formulaire* [1899, p. 30] osserva: «Vi è un'infinità di sistemi che soddisfano tutte le proprietà primitive [cioè gli assiomi P.1-P.5]. Esse risultano per esempio tutte verificate se si sostituiscono *numero* e 0 con *numero diverso da* 0 e 1». La stessa oscillazione di Peano e della sua scuola nel formulare gli assiomi per i naturali *senza* lo zero o *con* lo zero appare dunque nella sua vera luce: gli assiomi peaniani non assegnano ai numeri 0, 1, 2, 3, ecc. alcun significato, specificano soltanto che essi devono godere di certe proprietà enunciate dagli assiomi. Di piú la posizione di Peano sembra essere stata quella di considerare numero, zero e successore non solo come tre nozioni indefinite, ma come vere e proprie *indefinibili* [cfr. le osservazioni critiche di Russell 1903, trad. it. in particolare pp. 196-201]. Ma Peano, personalmente, fu sempre piuttosto restio a costruire una vera e propria filosofia sulla base di questo approccio. Non sono mancate però nel Novecento differenti versioni del formalismo, tutte unanimi nel concludere che *numero*, *zero* e *successore* sono semplicemente (ed esclusivamente) quel che è implicitamente definito dagli assiomi peaniani o da qualche loro variante. Bertrand Russell era solito paragonare costoro a degli orologiai cosí preoccupati della raffinatezza dei congegni da loro costruiti, da dimenticarsi che un orologio deve usualmente segnare le ore e che va quindi provvisto anche di un quadrante. Con terminologia diversa, si potrebbe dire che, se anche il punto di vista formalista ha successo nel ricostruire in larghissima misura la pratica del calcolo, sotto questo profilo soddisfa forse un'esigenza di «razionalità», ma non ancora un'esigenza di «intelligibilità»...

6.2. Lo zero nel contesto insiemistico. Definizione dell'insieme vuoto.

Un passo ulteriore viene compiuto con una tipica *riduzione* (cfr. per gli aspetti generali l'omonimo articolo in questa stessa *Enciclopedia*) della teoria dei naturali alla teoria degli insiemi. In quest'ultimo contesto, come si può vedere in altri articoli di questa stessa *Enciclopedia* (in particolare «Assioma/postulato» e «Insieme»), i numeri naturali vengono espressi come «potenze» o «numeri cardinali» di insiemi *finiti* (cfr. anche la reinterpretazione degli assiomi di Peano P.1-P.5 come P′.1-P′.5 nel citato articolo «Calcolo»). Lo zero risulta allora la «potenza» o «numero cardinale» dell'insieme vuoto (*empty set* nella terminologia corrente) o classe nulla (*null class* nel linguaggio delle classi) (cfr. del resto il citato articolo «Insieme», VII, p. 755).

Ma «le difficoltà di Fredegiso ricompaiono tutte, immediatamente, in quest'ultimo concetto, a proposito della sua definizione e della sua esistenza» [Geymonat 1952, ed. 1953 p. 105]. Se con il creatore della teoria degli insiemi, Georg Cantor, s'intende per classe o insieme (*Menge*: la successiva distinzione tra «insieme» e «classe», abituale al logico matematico dopo «la crisi dei fondamenti», non sarà esplicitamente richiamata o utilizzata qui) «l'unione in un tutto di oggetti distinti della nostra intuizione o del nostro pensiero» (cfr. del resto quanto osservato nel citato articolo «Insieme», § 1), che tipo di esistenza si dovrà attribuire alla classe *vuota* che appunto non «unisce in un tutto» alcun elemento? E «se essa non esiste, con che diritto potremo parlarne, come di fatto ne parliamo, in tutta la matematica?» [*ibid.*, pp. 105-6]. In linea teorica si potrebbe anche sostenere che è bene fare a meno della classe nulla (dunque anche dello zero, o almeno di una interpretazione che lo renda «intelligibile»). Ma una soluzione cosí «reazionaria» (per usare le parole di Russell [1903, trad. it. p. 130]) riporterebbe all'antica ambiguità (zero: segno di mancanza o mancanza di segno?), in contrasto però con la stessa pratica del calcolo cosí come si è venuta via via articolando.

Una celebre via per eludere esiti cosí drastici, risalente sostanzialmente a Frege [1884] consiste nel modificare l'«archetipo» cantoriano di insieme. Dare una classe M non vuol piú dire, come pretendeva Cantor, dare un raggruppamento: vuol dire invece precisare una regola di appartenenza, determinare cioè per ogni x se x appartenga o non appartenga a M. Ora, perché escludere una regola tipo 'Per ogni x, x non appartiene a M'? Questa regola può venir suggerita da qualsiasi concetto contraddittorio, per esempio «disuguale da se stesso». Se infatti si pone 'x appartiene a M se e solo se $x \neq x$', si trova immediatamente la classe vuota [per un riepilogo della questione cfr. Bunn 1980, pp. 226-31].

Com'è noto, l'originaria versione fregeana delle classi è stata modificata dopo la scoperta di celebri antinomie: è però facile riadattare il procedimento di Frege piú sopra delineato a una qualche teoria assiomatica degli insiemi, come per esempio alla versione di Zermelo, Fraenkel e Skolem (per cui si vedano i citati articoli «Assioma/postulato» e «Insieme»: qui, grazie al cosiddetto «principio di isolamento» o «assioma del sottoinsieme», è possibile de-

finire un insieme vuoto *isolando* in un dato insieme A l'insieme M con la condizione $x \neq x$. Sarà poi immediato mostrare che tale insieme M è unico utilizzando il principio di estensionalità [cfr. per esempio Fraenkel e Bar-Hillel 1958, pp. 42-43; cfr. anche per un approccio lievemente differente il citato articolo «Assioma/postulato», in particolare § 4].

Per questa via si potrebbe anche concludere che la «regola» su accennata «fornisce la definizione operativa (di un operativismo matematico, s'intende!) della classe vuota e quindi dello zero, e riesce con ciò a risolvere appieno le difficoltà di principio che sembravano legate a questo fondamentale concetto della scienza» [Geymonat 1952, ed. 1953 p. 106]. L'autore del presente articolo è però d'accordo con una valutazione del genere solo per la prima metà: infatti che tale definizione «operativa» dissolva «appieno» le difficoltà concettuali legate allo zero è per lo meno discutibile: dopo tutto in una teoria assiomatico-formale come quella di Zermelo, Fraenkel e Skolem si sa solo che esiste un insieme che *non* ha elementi (quello che tecnicamente è talvolta detto «un atomo») e che di tali «atomi» ve n'è uno solo (cfr. per esempio quanto osservato da Fraenkel e Bar-Hillel [1958, pp. 31 e 42-43]: va anche detto che in certe varianti della teoria si possono anche ammettere piú «atomi» differenti, con risultati tecnici di notevole interesse; la questione non sarà però affrontata qui). Una volta abbandonato l'archetipo cantoriano, resta dunque il problema d'individuarne un altro, che permetta di ritrovare l'intelligibilità dei passi formali compiuti.

Una soluzione del genere è stata già individuata da Russell e benché essa comporti una notevole complicazione rispetto alla dottrina che associa a un concetto la classe degli individui che tale concetto soddisfano, varrà la pena di accennarvi nelle pagine che immediatamente seguono anche per il fatto che essa permetterà di specificare la natura dei cosiddetti «zeri puri di grandezza» di cui si tratterà nel § 7.

6.3. Russell, i concetti classe e la classe nulla.

«È chiaro, – scrive Russell [1903], – che esiste un concetto quale il *nulla*, e che in un certo senso nulla è qualcosa. In realtà la proposizione "il nulla non è nulla" è senza alcun dubbio suscettibile di un'interpretazione che la rende vera» (trad. it. p. 128). Riappare ancora l'argomento di Fredegiso (cfr. § 2) e, risalendo nella tradizione del pensiero occidentale, tutta la tematica del non essere discussa già da Platone, in ispecie nel *Sofista* [in particolare 254 sgg.]. Per esempio: «LO STRANIERO Come hai detto, ciò non è inferiore, quanto all'essere, a nessuna altra cosa. E non occorre dire ormai coraggiosamente che "ciò che non è" è saldamente ed ha una sua propria natura, come vedemmo che il grande è grande, e che il bello è bello, e ciò che non è grande non-grande, e ciò che non è bello non-bello? Anche "ciò che non è", per la stessa ragione, vedemmo essere, ed è non essendo, ed è un genere da annoverare fra i molti altri che sono. Oppure, Teeteto, v'è ancora qualche perplessità in ciò? TEET. Nessuna. LO STR. Lo sai che noi abbiamo abbandonato Parmenide e siamo

andati assai al di là del suo divieto? TEET. E perché? LO STR. Piú di quello ch'egli ci proibí di prendere in esame, noi ricercammo, procedendo oltre il limite e anche piú avanti, e gliene demmo dimostrazione. TEET. Ma come fu? LO STR. Perché egli in qualche luogo dice: "Tu infatti mai costringerai ad essere ciò che non è, | tu invece da questa via, nel tuo cercare, tieni lontano il pensiero"» [*ibid.*, 258b-d].

Ora, «*nulla* è un concetto denotante che non denota alcunché... La proposizione... riferita, che sembra cosí paradossale, non significa altro che questo: *nulla*, il concetto denotante, non è un nulla, cioè non è ciò che esso stesso denota» [Russell 1903, trad. it. p. 131]. Questa mossa comporta la seguente difficoltà. Si considerino, per esempio, proposizioni come 'Le chimere sono animali'. «A prima vista, – commenta Russell, – queste proposizioni sembrano vere, e parrebbe che esse non si riferiscano ai concetti denotanti, ma a ciò che questi concetti denotano; eppure ciò è impossibile, poiché i concetti in questione non denotano alcunché. La logica simbolica dice che questi concetti denotano la classe-nulla, e che [tali] proposizioni... asseriscono che la classe-nulla è contenuta in certe altre classi. Ma... una classe che non abbia termini non può assolutamente essere qualcosa: ciò che è puramente e semplicemente una collezione di termini [cfr. quanto si è detto a p. 1345], non può sussistere quando i termini siano tolti» [*ibid.*, p. 129]. Ciò richiede una «correzione» che può venir brevemente schematizzata come segue.

Tutti i concetti denotanti, osserva ancora Russell, derivano da *concetti classe*: a è un concetto classe quando 'x è un a' è una funzione proposizionale, una «funzione» cioè che assume i valori di verità 'vero' o 'falso' a ogni sostituzione della variabile x con una costante. Ora «i concetti denotanti uniti ad a non denoteranno alcunché quando e soltanto quando "x è un a" risulta falsa per tutti i valori di x» [*ibid.*]. Tali concetti classe verranno battezzati «concetti classe nulli». Il riferimento della classe nulla sarà allora la classe di tutti i concetti nulli, oppure la classe di tutte le funzioni proposizionali nulle. «Se quindi vogliamo avere una entità analoga a quella che altrimenti si chiamerebbe classe, ma corrispondente ai concetti-classe nulli, siamo costretti... ad introdurre un termine che risulti identico per concetti-classe uguali, ed a sostituire dappertutto la classe dei concetti-classe uguali ad un dato concetto-classe, alla classe corrispondente a quel concetto-classe... La classe-nulla, in effetti, è in qualche modo analoga ad un irrazionale in aritmetica: non può cioè venir interpretata secondo gli stessi principi che servono per le altre classi, e se noi vogliamo darne un'interpretazione analoga in sede diversa, dobbiamo sostituire alle classi altre entità piú complicate» [*ibid.*, p. 131].

7. *Lo «zero puro di grandezza»: Russell a proposito di Kant e Meinong.*

Accettando la soluzione del paragrafo precedente – in particolare la variante proposta da Russell –, il problema del non essere che «lo straniero», protagonista del *Sofista*, formula «procedendo oltre il limite» posto da Parmenide, per quanto

riguarda il contesto delle matematiche sembra avviato se non a soluzione, a una chiarificazione. Ma che portata può avere tale chiarificazione fuori dal contesto delle matematiche? In altri termini, è essa in qualche modo esemplare? E del resto, con lo stabilirsi di una «corretta» grammatica per il termine zero entro la logica formale e le matematiche, qual è l'entità dello slittamento avvenuto?

Saranno ancora le parole di un filosofo a far da guida, nella fattispecie la confutazione kantiana dell'argomento che Moses Mendelssohn aveva esposto nel suo *Fedone, o L'immortalità dell'anima* (*Phädon, oder die Unsterblichkeit der Seele*, 1767). Per Mendelssohn l'anima è un essere *semplice*, senza parti o molteplicità, e come tale non può venir «decomposto» e quindi cessare di esistere. Ma, ribatte Kant nella *Critica della ragion pura* [1787], «questo perspicace filosofo... non tenne conto del fatto che, anche concedendo all'anima una natura semplice del genere, per cui essa non racchiude alcuna molteplicità di parti reciprocamente esterne, perciò alcuna quantità estensiva, non è tuttavia possibile negarle, come a ogni altra cosa esistente, una quantità intensiva, ossia un grado di realtà rispetto ad ognuna delle sue facoltà, anzi, in generale, rispetto a tutto ciò che ne costituisce l'esistenza; questo grado può andar diminuendo attraverso un numero infinito di gradi sempre piú piccoli, sicché la pretesa sostanza potrà ridursi a nulla, se non per decomposizione, per un progressivo sminuimento (*remissio*) delle sue forze (quindi per illanguidimento, se mi è concesso l'impiego d'una espressione del genere). La coscienza, infatti, ha sempre un grado, suscettibile di venir diminuito, e lo stesso dicasi della facoltà di esser coscienti di sé, e di tutte le altre facoltà» (trad. it. pp. 340, 341).

L'obiezione kantiana fa dunque riferimento al cosiddetto «zero puro di grandezza». Ma come va definito questo? Russell [1903] esamina la definizione tradizionale dello zero di un genere di grandezza come «minima grandezza del suo genere» (trad. it. pp. 272-77). Sia nel caso di una grandezza discreta che nel caso di una continua (cfr. l'articolo «Continuo/discreto» in questa stessa *Enciclopedia*) tale definizione si rivela inadeguata.

a) *Caso discreto*: sia lo zero che dovrebbe funzionare da «grandezza limitante» la minima del suo genere. Ma allora l'enunciato che lo zero è la minore delle grandezze è simile all'enunciato 'Achille era il piú forte di tutti i suoi nemici'. Enunciato «retorico», in quanto tutti i nemici di Achille sono *meno* forti di Achille e non si può verosimilmente considerare Achille nemico di se stesso. Analogamente «sarebbe ovviamente falso dire che lo zero sia il minimo degli interi positivi, o che l'intervallo tra *A* ed *A* sia il minimo intervallo tra due lettere qualsiasi dell'alfabeto» [*ibid.*, p. 274].

b) *Caso continuo*: se «le nostre grandezze sono... delle distanze, lo zero possiede, a prima vista, un significato ovvio, e precisamente l'identità» [*ibid.*]. Questa eventualità è un tipico caso esemplare in cui la filosofia dell'identità diventa un caso *limite* della filosofia della differenza. Piú in generale «in qualunque classe di grandezze che sia continua... possiamo introdurre lo zero nello stesso modo con cui si ottengono i numeri reali dai razionali» [*ibid.*, p. 275]. Dando opportunamente «numeri alle cose» (cfr. quanto osservato nell'articolo «Numero» in questa stessa *Enciclopedia*, al § 7) si potranno correlare

i vari «gradi» della grandezza in questione a numeri *razionali* e costruire una successione (cfr. il «numero infinito di gradi sempre piú piccoli» di cui parla Kant) che sia una cosiddetta «zero-successione» o «successione di Cauchy» per «definire» lo zero di quella grandezza. Qui non sussiste «un approssimarsi discreto alla classe nulla... tale approssimarsi è (nei diversi sensi della parola) continuo». Si tratta certo dello *zero di quella grandezza*, ma in un senso pickwickiano: di fatto «questo metodo rende... lo zero identico per tutti i generi di grandezza, e non ne fa una tra le grandezze di cui esso è lo zero» [*ibid.*].

Proprio quando si dice che l'identità è un caso limite della differenza, se non si vuole fare della mera retorica, si deve ricordare che il limite *non* è *omogeneo* alla successione di cui è limite. Come sa ogni studente di analisi quando ha a che fare con il postulato della continuità (cfr. il citato articolo «Calcolo», II, pp. 416-18), una successione di segmenti ciascuno compreso nel precedente individua un punto, ma un *punto* non è un *segmento*. Di nuovo la locuzione che lo zero è il minimo di una grandezza appare inadeguata. Fin dal caso esemplare delle distanze si deve dunque riqualificare tutta «la filosofia» precedente notando «che una distanza-zero è puramente e semplicemente *nessuna distanza*» [*ibid.*, p. 276].

Nella questione si affronta cosí «il problema della natura della negazione» [*ibid.*, p. 275; cfr. le osservazioni di Geymonat 1952, ed. 1953 p. 107]. Un passo interessante è allora quello compiuto da Meinong nel suo *Sul significato della legge di Weber*, là dove lo zero di un genere di quantità viene introdotto come «l'opposto contraddittorio» di ogni grandezza del genere considerato [1896, p. 8]. Ancora una volta la critica di Russell [1903, trad. it. pp. 252-53, 272-73, 276-77] svela però alcune ambiguità. Nel calcolo delle classi dell'usuale pratica logica e matematica (cfr. ancora «Calcolo», II, pp. 396-400) l'«opposto» (o «complemento») di una classe è la classe contenente tutti gli elementi di un dato «universo» che non appartengono alla classe data. Ora questo riferimento «è evidentemente non appropriato; non è vero che lo zero sia ogni cosa eccetto una grandezza del suo genere, e neppure che sia ogni cosa eccetto la classe delle grandezze del suo genere. Si può difficilmente considerare vera l'affermazione che un dolore sia un piacere zero» [*ibid.*, p. 273].

A un piú attento esame Meinong [1896] sembra invece sostenere che un piacere zero è in realtà nessun piacere, il che non coincide affatto con *non* piacere. 'Zero piacere' (ovvero 'nessun piacere') «sembra voler dire che un piacere zero non è né piacere né alcun'altra cosa», conclude Russell e commenta: «Un modo scomodo di dire *nulla*, [mentre] il riferimento al piacere dovrebbe essere lasciato completamente da parte» [1903, trad. it. p. 273]. Si è dunque camminato in circolo, movendo dalla croce delle ontologie, cioè del non-essere espresso dagli zeri puri (zero puro di distanza, zero puro di piacere, ma anche – perché no? – zero puro di esistenza) per ritrovarsi con il nulla, puro non-essere (cfr. anche le osservazioni fatte all'inizio e *passim* nell'articolo «Metafisica» in questa stessa *Enciclopedia*)? Forse sí: ma è stato un circolo *virtuoso*, in cui qualcosa pure si è appreso. E cosa? La relazione «singolare e intima» di un concetto come zero piacere con la negazione logica: «Non esiste alcuna

quantità la cui *grandezza* sia zero, cosicché la classe delle quantità zero è la classe nulla» [*ibid.*, pp. 276-77]. Gli zeri puri di grandezza (in particolare lo stesso zero puro di esistenza, erede della versione ontologica del *nihil* di Fredegiso, cfr. § 2) restano, «propriamente parlando», degli indefinibili, «come le altre grandezze del genere» [*ibid.*, p. 277] ma possono venir specificati grazie a questa relazione con lo zero delle matematiche, piú propriamente con la classe nulla.

8. *Zero come «adombramento».*

Ci si potrebbe arrestare qui: e non certo perché le considerazioni svolte in precedenza (§§ 6 e 7) esauriscano «l'abisso» sottostante allo zero ma perché deve pur esserci un termine all'esposizione del gioco dei problemi e delle congetture che s'intrecciano intorno a un particolare nodo. Ma, anche tenendo conto del fatto che, per una bizzarria alfabetica, con l'articolo «Zero» termina questa *Enciclopedia* (ovvero questo viaggio, in cui un qualche Ulisse si lascia alle spalle un mare popolato di strani «mostri», ma quale Itaca può mai aspettarlo?), sia lecito a chi scrive proporre ancora un'ultima citazione.

Dai *Sonnambuli* (*Die Schlafwandler*, 1931-32) di Hermann Broch: «L'assassinio resta assassinio, la malvagità resta malvagità, e il filisteismo di una sfera di valori limitata all'individuo e ai suoi impulsi irrazionali, questo prodotto estremo di ogni disgregazione dei valori, resta il punto dell'abiezione assoluta, resta, in certo modo, lo zero, l'invariante assoluto, che, prescindendo dalla loro reciproca relatività, è comune, e tale dev'essere, a tutte le scale e a tutti i sistemi del valore, perché non se ne può fondare alcuno che nella sua idea e nella sua essenza logica non sia soggetto alla "condizione dell'esperienza possibile": empirico adombramento di una struttura logica comune a tutti i sistemi e di un'aprioristica immutabilità connessa con il logos. E sembra quasi discendere dalla stessa necessità logica che il passaggio dal vecchio al nuovo sistema debba compiersi attraverso quello zero in cui si atomizzano i valori, attraverso una generazione che, priva di ogni rapporto col vecchio e col nuovo sistema, appunto in questa mancanza di rapporti... giustifica, dal punto di vista etico e storico, lo spietato disprezzo cui viene esposto tutto ciò che è umano in tempi di rivoluzione» [III, 88].

L'autore del presente articolo non ritiene opportuno alcun commento per queste parole (ovvero, nella sede costituita dall'*Enciclopedia* esse si commentano benissimo da sé). Sia lecito aggiungere solo che esse esprimono un suo *feeling*, strettamente personale, una sorta di erosione interna prodotta dall'inquietudine. [G. G.].

Badiou, A.
1969 *Marque et manque: à propos du zéro*, in «Cahiers pour l'analyse», n. 10, pp. 150-73.
Bayes, Th.
1736 *An Introduction to the Doctrine of Fluxions*, Noon, London.

Berkeley, G.
1734 *The Analyst; or, a Discourse Addressed to an Infidel Mathematician*, Tonson, London (trad. it. Fondazione Giorgio Ronchi, Firenze 1971).
Black, M.
1977 «Zero», in *Encyclopaedia Americana*, vol. XXIX, Americana Corporation, New York, pp. 770-71.
Bledsoe, A. T.
1867 *The Philosophy of Mathematics*, Lippincott, Philadelphia.
Boyer, C. B.
1943 *An early reference to division by zero*, in «The American Mathematical Monthly», L, pp. 487-91.
1968 *A History of Mathematics*, Wiley, New York (trad. it. Isedi, Milano 1976).
Bunn, R.
1980 *Developments in the Foundations of Mathematics 1870-1910*, in I. Grattan-Guinness (a cura di), *From Calculus to Set Theory. An Introductory History*, Duckworth, London, pp. 220-55.
Cajori, F.
1928 *A History of Mathematical Notations*, I. *Notations in Elementary Mathematics*, Open Court, Chicago.
1929 *A History of Mathematical Notations*, II. *Notations Mainly in Higher Mathematics*, Open Court, Chicago.
Cohn, P. M.
1965 *Universal Algebra*, Harper and Row, New York (trad. it. Feltrinelli, Milano 1971).
Courant, R., e Robbins, H.
1941 *What is Mathematics?*, Oxford University Press, London - New York (trad. it. Boringhieri, Torino 1972²).
Court de Gébelin, A.
1773-82 *Du jeu des tarots*, in *Monde primitif, analysé et comparé avec le monde moderne*, Chez l'auteur, Paris (trad. it. Ottaviano, Milano 1981).
Couturat, L.
1896 *De l'Infini mathématique*, Alcan, Paris.
Eulero, L.
1755 *Institutiones calculi differentialis cum eius usu in analysi finitorum ac doctrina serierum*, Impensis Academiae Imperialis Scientiarum Petropolitanae; ora in *Opera omnia*, serie I, vol. X, Teubner, Leipzig-Berlin 1913.
1770 *Vollständige Anleitung zur Algebra*, Kayserliche Akademie der Wissenschaften, Sankt Petersburg.
Fraenkel, A. A., e Bar-Hillel, Y.
1958 *Foundations of Set Theory*, North Holland, Amsterdam.
Frege, G.
1884 *Die Grundlagen der Arithmetik. Eine logisch-mathematische Untersuchung über den Begriff der Zahl*, Köbner, Breslau (trad. it. in *Logica e aritmetica*, Boringhieri, Torino 1977², pp. 207-349).
Geymonat, L.
1952 *I problemi del nulla e delle tenebre in Fredegiso di Tours*, in «Rivista di filosofia», XLIII, 3, pp. 280-88; ora in *Saggi di filosofia neorazionalistica*, Einaudi, Torino 1953, pp. 101-11.
Gilson, E.
1944 *La philosophie au Moyen Age. Des origines patristiques à la fin du XIVe siècle*, Payot, Paris 1944² (trad. it. La Nuova Italia, Firenze 1973).
Heath, Th. L.
1931 *A Manual of Greek Mathematics*, Clarendon Press, Oxford; ed. Dover, New York 1963.
Hegel, G. W. F.
1812-16 *Wissenschaft der Logik*, 3 voll., Schrag, Nürnberg (trad. it. Laterza, Bari 1974³).

Hill, G. F.
1915 *The Development of Arabic Numerals in Europe*, Clarendon Press, Oxford.

Humboldt, A. von
1829 *Über die bei verschiedenen Völkern üblichen Systeme von Zahlzeichen und über den Ursprung des Stellenwerthes in den indischen Zahlen*, in «Journal für die reine und angewandte Mathematik», IV, 3, pp. 205-31.

Ifrah, G.
1981 *Histoire universelle des chiffres*, Seghers, Paris.

Jordan, L.
1905 *Materialien zur Geschichte der arabischen Zahlzeichen in Frankreich*, in «Archiv für Kulturgeschichte», III, pp. 155-95.

Kant, I.
1787 *Kritik der reinen Vernunft*, Hartknoch, Riga 1787[2] (trad. it. Utet, Torino 1967).

Kline, M.
1972 *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York.
1980 *Mathematics. The Loss of Certainty*, Oxford University Press, New York.

Laing, R. D.
1976 *The Facts of Life*, Pantheon Books, New York (trad. it. Einaudi, Torino 1978).

Meinong, A.
1896 *Über die Bedeutung des Weberschen Gesetzes*, Voss, Hamburg-Leipzig.

Menninger, K. W.
1957 *Zahlwort und Ziffer*, Vandenhoeck und Ruprecht, Göttingen (trad. ingl. Mit Press, Cambridge Mass. 1977[2]).

Meschkowski, H.
1960 *Wandlungen des mathematischen Denkens*, Vieweg, Braunschweig 1960[2] (trad. it. Boringhieri, Torino 1973[2]).

Morini, S.
1980 *Attraverso uno specchio scuro. Enigmi e problemi secondo Feyerabend*, in «L'uomo, un segno», IV, 2-3, pp. 181-97.

Neugebauer, O.
1957 *The Exact Sciences in Antiquity*, Brown University Press, Providence R.I. 1957[2] (trad. it. Feltrinelli, Milano 1974).

Peano, G.
1899 *Formulaire de Mathématiques*, II, § 3, Bocca e Clausen, Torino.

Russell, B.
1903 *The Principles of Mathematics*, Cambridge University Press, Cambridge (trad. it. Longanesi, Milano 1963).

Smith, D. E.
1923 *History of Mathematics*, I. *General Survey of the History of Elementary Mathematics*, Ginn, Boston - New York; ed. Dover, New York 1958.
1925 *History of Mathematics*, II. *Special Topics of Elementary Mathematics*, Ginn, Boston - New York; ed. Dover, New York 1958.

Smith, D. E., e Karpinski, L. Ch.
1911 *The Hindu-Arabic Numerals*, Ginn, Boston.

Struik, D. J.
1967 *A Concise History of Mathematics*, Dover, New York 1967[3].

Suppes, P. C.
1957 *Introduction to Logic*, Van Nostrand, Princeton N.J.

Vasoli, C.
1961 *La filosofia medievale*, Feltrinelli, Milano.

Waerden, B. L. van der
1961 *Science Awakening*, Oxford University Press, New York.

Rappresentazione stessa dell'**ambiguità**, in quanto inteso ora come mancanza di **segno** ora come **simbolo** per il nulla, lo zero è slittato da semplice operatore aritmetico a ente (cfr. **essere**) dotato di proprietà determinate, modificando in tal modo il concetto stesso di **numero**. È in particolare il passaggio dal computo con l'**abaco**, ove lo zero è semplicemente un posto vuoto, a un **calcolo** scritto (cfr. anche **scrittura**) che ha fatto sí che questo ente ambiguo sia divenuto sempre piú necessario in piú di un **algoritmo**. All'interno delle **matematiche**, le sue proprietà piú generali sono emerse nel contesto delle varie **strutture matematiche**, mentre la giustificazione della sua **esistenza** si è riproposta dal punto di vista della moderna **formalizzazione** (cfr. anche **assioma/postulato**) per trovare risposta nel quadro della teoria degli insiemi (cfr. **insieme**). L'analisi promossa dalla **logica** della nozione di zero ha costituito infine un **paradigma** per la trattazione del problema tipicamente filosofico (cfr. **filosofia/filosofie, metafisica**) dei cosiddetti «zeri puri» delle grandezze, sia discrete sia continue (cfr. **continuo/discreto**), permettendo cosí un'articolazione soddisfacente di una teoria delle quantità (cfr. **qualità/quantità**) e giovando allo sviluppo di una filosofia della differenza (cfr. **identità/differenza**).